Gerenciamento de STORAGE SAN

ONTAP 9

NetApp
January 17, 2025

Índice

Gerenciamento de STORAGE SAN

Conceitos de SAN

Provisionamento DE SAN com iSCSI

Em ambientes SAN, os sistemas de armazenamento são alvos que têm dispositivos de armazenamento de destino. Para iSCSI e FC, os dispositivos de destino de armazenamento são referidos como LUNs (unidades lógicas). Para Non-Volatile Memory Express (NVMe) em Fibre Channel, os dispositivos de destino de storage são chamados de namespaces.

Você configura o storage criando LUNs para iSCSI e FC ou criando namespaces para NVMe. Os LUNs ou namespaces são então acessados por hosts que usam redes de protocolo iSCSI (Internet Small Computer Systems Interface) ou Fibre Channel (FC).

Para se conetar a redes iSCSI, os hosts podem usar placas de rede Ethernet (NICs) padrão, TOE (TCP offload Engine) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host iSCSI dedicados (HBAs).

Para se conetar a redes FC, os hosts exigem HBAs FC ou CNAs.

Os protocolos FC compatíveis incluem:

- FC
- FCoE
- NVMe

Ligações e nomes de rede de nó de destino iSCSI

Os nós de destino iSCSI podem se conetar à rede de várias maneiras:

- Interfaces over Ethernet usando software integrado ao ONTAP.
- Em várias interfaces de sistema, com uma interface usada para iSCSI que também pode transmitir tráfego para outros protocolos, como SMB e NFS.
- Usando um adaptador de destino unificado (UTA) ou um adaptador de rede convergente (CNA).

Cada nó iSCSI deve ter um nome de nó.

Os dois formatos, ou designadores de tipo, para nomes de nós iSCSI são *iqn* e *eui*. O destino SVM iSCSI sempre usa o designador do tipo iqn. O iniciador pode usar o designador iqn-type ou eui-type.

Nome do nó do sistema de storage

Cada SVM que executa iSCSI tem um nome de nó padrão com base em um nome de domínio reverso e um número de codificação exclusivo.

O nome do nó é exibido no seguinte formato:

iqn.1992-08.com.NetApp:sn.*unique-encoding-number*

O exemplo a seguir mostra o nome do nó padrão para um sistema de armazenamento com um número de codificação exclusivo:

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

Porta TCP para iSCSI

O protocolo iSCSI está configurado no ONTAP para utilizar a porta TCP número 3260.

O ONTAP não suporta a alteração do número da porta para iSCSI. A porta número 3260 está registada como parte da especificação iSCSI e não pode ser utilizada por qualquer outra aplicação ou serviço.

Informações relacionadas

"Documentação do NetApp: Configuração do host SAN ONTAP"

Gerenciamento de serviços iSCSI

Gerenciamento de serviços iSCSI

Você pode gerenciar a disponibilidade do serviço iSCSI nas interfaces lógicas iSCSI da máquina virtual de storage (SVM) usando os `vserver iscsi interface enable` comandos ou `vserver iscsi interface disable`.

Por predefinição, o serviço iSCSI está ativado em todas as interfaces lógicas iSCSI.

Como o iSCSI é implementado no host

O iSCSI pode ser implementado no host usando hardware ou software.

Você pode implementar iSCSI de uma das seguintes maneiras:

- Usando o software Initiator que usa as interfaces Ethernet padrão do host.
- Através de um adaptador de barramento de host iSCSI (HBA): Um HBA iSCSI aparece para o sistema operacional do host como um adaptador de disco SCSI com discos locais.
- Usando um adaptador TOE (TCP Offload Engine) que descarrega o processamento TCP/IP.

  O processamento do protocolo iSCSI ainda é realizado pelo software anfitrião.

Como a autenticação iSCSI funciona

Durante a fase inicial de uma sessão iSCSI, o iniciador envia uma solicitação de login ao sistema de armazenamento para iniciar uma sessão iSCSI. O sistema de armazenamento permite ou nega a solicitação de login ou determina que não é necessário fazer login.

Os métodos de autenticação iSCSI são:

- Challenge Handshake Authentication Protocol (CHAP) - o iniciador faz login usando um nome de usuário e senha CHAP.

Você pode especificar uma senha CHAP ou gerar uma senha secreta hexadecimal. Existem dois tipos de nomes de usuário CHAP e senhas:

  - Entrada - o sistema de armazenamento autentica o iniciador.

    As configurações de entrada são necessárias se você estiver usando a autenticação CHAP.

  - Outbound — esta é uma configuração opcional para permitir que o iniciador autentique o sistema de armazenamento.

    Só pode utilizar as definições de saída se definir um nome de utilizador e uma palavra-passe de entrada no sistema de armazenamento.

- Negar - o iniciador tem acesso negado ao sistema de armazenamento.
- Nenhum - o sistema de storage não requer autenticação para o iniciador.

Pode definir a lista de iniciadores e os respetivos métodos de autenticação. Você também pode definir um método de autenticação padrão que se aplica a iniciadores que não estão nesta lista.

Informações relacionadas

"Opções de multipathing do Windows com Data ONTAP: Fibre Channel e iSCSI"

Gerenciamento de segurança do iniciador iSCSI

O ONTAP fornece uma série de recursos para gerenciar a segurança para iniciadores iSCSI. Pode definir uma lista de iniciadores iSCSI e o método de autenticação para cada um, apresentar os iniciadores e os respetivos métodos de autenticação associados na lista de autenticação, adicionar e remover iniciadores da lista de autenticação e definir o método de autenticação do iniciador iSCSI predefinido para iniciadores que não estão na lista.

Isolamento do ponto de extremidade iSCSI

A partir do ONTAP 9.1, os comandos de segurança iSCSI existentes foram melhorados para aceitar um intervalo de endereços IP ou vários endereços IP.

Todos os iniciadores iSCSI devem fornecer endereços IP de origem ao estabelecer uma sessão ou conexão com um destino. Essa nova funcionalidade impede que um iniciador faça login no cluster se o endereço IP de origem não for suportado ou desconhecido, fornecendo um esquema de identificação exclusivo. Qualquer iniciador originado de um endereço IP não suportado ou desconhecido terá seu login rejeitado na camada de sessão iSCSI, impedindo que o iniciador acesse qualquer LUN ou volume dentro do cluster.

Implemente essa nova funcionalidade com dois novos comandos para ajudar a gerenciar entradas pré-existentes.

Adicionar intervalo de endereços do iniciador

Melhore o gerenciamento de segurança do iniciador iSCSI adicionando um intervalo de endereços IP ou vários endereços IP com o `vserver iscsi security add-initiator-address-range` comando.

```
cluster1::> vserver iscsi security add-initiator-address-range
```

Remova o intervalo de endereços do iniciador

Remova um intervalo de endereços IP ou vários endereços IP com o `vserver iscsi security remove-initiator-address-range` comando.

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

O que é a autenticação CHAP

O CHAP (Challenge Handshake Authentication Protocol) permite a comunicação autenticada entre iniciadores e destinos iSCSI. Quando você usa autenticação CHAP, você define nomes de usuário CHAP e senhas tanto no iniciador quanto no sistema de armazenamento.

Durante a fase inicial de uma sessão iSCSI, o iniciador envia uma solicitação de login ao sistema de armazenamento para iniciar a sessão. A solicitação de login inclui o nome de usuário CHAP do iniciador e o algoritmo CHAP. O sistema de armazenamento responde com um desafio CHAP. O iniciador fornece uma resposta CHAP. O sistema de armazenamento verifica a resposta e autentica o iniciador. A senha CHAP é usada para calcular a resposta.

Diretrizes para o uso da autenticação CHAP

Você deve seguir certas diretrizes ao usar a autenticação CHAP.

- Se definir um nome de utilizador e uma palavra-passe de entrada no sistema de armazenamento, tem de utilizar o mesmo nome de utilizador e palavra-passe para as definições CHAP de saída no iniciador. Se também definir um nome de utilizador e uma palavra-passe de saída no sistema de armazenamento para ativar a autenticação bidirecional, tem de utilizar o mesmo nome de utilizador e palavra-passe para as definições CHAP de entrada no iniciador.
- Você não pode usar o mesmo nome de usuário e senha para configurações de entrada e saída no sistema de armazenamento.
- Os nomes de usuário CHAP podem ser de 1 a 128 bytes.

  Um nome de usuário nulo não é permitido.

- As senhas CHAP (segredos) podem ter 1 a 512 bytes.

  As senhas podem ser valores hexadecimais ou strings. Para valores hexadecimais, você deve inserir o valor com um prefixo "'0x'" ou "'0x'". Não é permitida uma palavra-passe nula.

> O ONTAP permite o uso de carateres especiais, letras não inglesas, números e espaços para senhas CHAP (segredos). No entanto, isso está sujeito a restrições de host. Se algum destes não for permitido pelo seu anfitrião específico, não poderão ser utilizados.
>
> Por exemplo, o iniciador de software iSCSI da Microsoft requer que as senhas CHAP do iniciador e do destino tenham pelo menos 12 bytes se a criptografia IPsec não estiver sendo usada. O comprimento máximo da senha é de 16 bytes, independentemente de o IPsec ser usado.
>
> Para restrições adicionais, você deve ver a documentação do iniciador.

Como usar listas de acesso à interface iSCSI para limitar as interfaces do iniciador pode aumentar o desempenho e a segurança

As listas de acesso à interface ISCSI podem ser usadas para limitar o número de LIFs em uma SVM que um iniciador pode acessar, aumentando assim a performance e a segurança.

Quando um iniciador inicia uma sessão de descoberta usando um comando iSCSI `SendTargets`, ele recebe os endereços IP associados ao LIF (interface de rede) que está na lista de acesso. Por padrão, todos os iniciadores têm acesso a todas as LIFs iSCSI na SVM. Você pode usar a lista de acesso para restringir o número de LIFs em uma SVM a que um iniciador tem acesso.

Serviço de nomes de armazenamento de Internet (iSNS)

O iSNS (Internet Storage Name Service) é um protocolo que permite a deteção e o gerenciamento automatizados de dispositivos iSCSI em uma rede de armazenamento TCP/IP. Um servidor iSNS mantém informações sobre dispositivos iSCSI ativos na rede, incluindo seus endereços IP, nomes de nós iSCSI IQN e grupos de portais.

Você pode obter um servidor iSNS de um fornecedor terceirizado. Se você tiver um servidor iSNS na rede configurado e habilitado para uso pelo iniciador e destino, poderá usar o LIF de gerenciamento de uma máquina virtual de armazenamento (SVM) para Registrar todos os LIFs iSCSI para esse SVM no servidor iSNS. Depois que o Registro estiver concluído, o iniciador iSCSI pode consultar o servidor iSNS para descobrir todos os LIFs para esse SVM específico.

Se você decidir usar um serviço iSNS, deve garantir que suas máquinas virtuais de armazenamento (SVMs) estejam registradas corretamente em um servidor iSNS (Internet Storage Name Service).

Se você não tiver um servidor iSNS na rede, você deverá configurar manualmente cada destino para ser visível para o host.

O que um servidor iSNS faz

Um servidor iSNS usa o protocolo iSNS (Internet Storage Name Service) para manter informações sobre dispositivos iSCSI ativos na rede, incluindo seus endereços IP, nomes de nós iSCSI (IQNs) e grupos de portais.

O protocolo iSNS permite a deteção e o gerenciamento automatizados de dispositivos iSCSI em uma rede de armazenamento IP. Um iniciador iSCSI pode consultar o servidor iSNS para descobrir dispositivos de destino iSCSI.

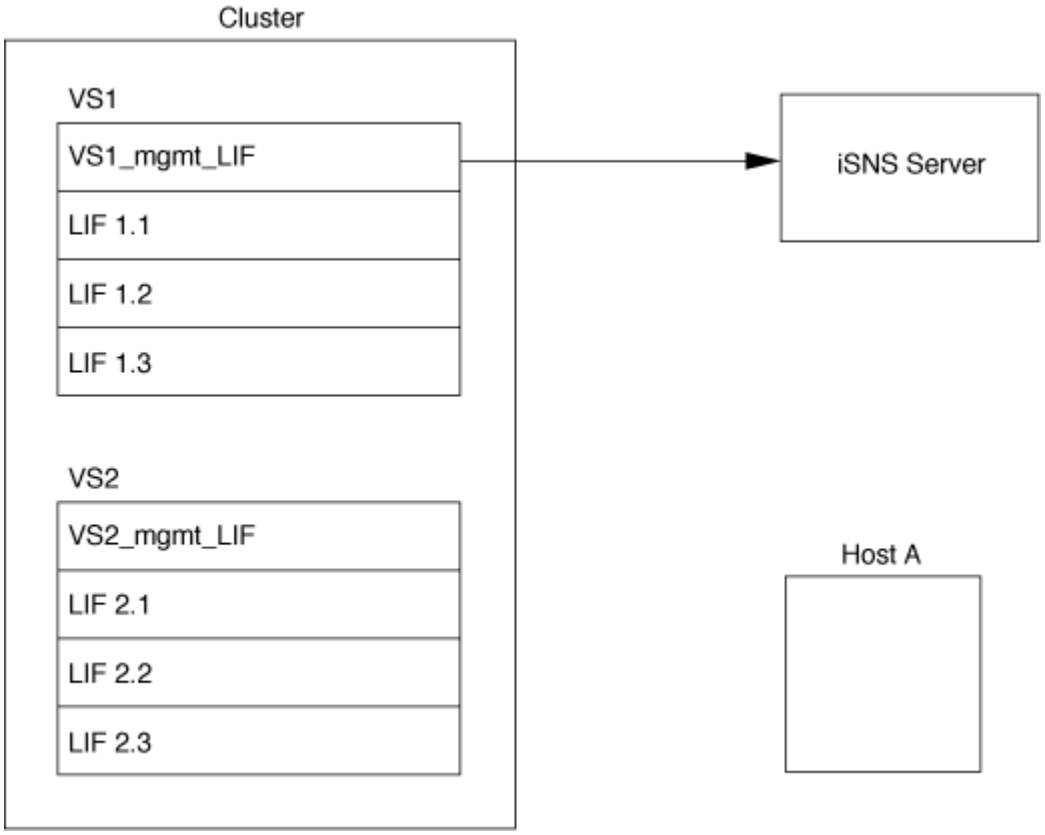
A NetApp não fornece ou revender servidores iSNS. Você pode obter esses servidores de um fornecedor suportado pelo NetApp.

Como os SVMs interagem com um servidor iSNS

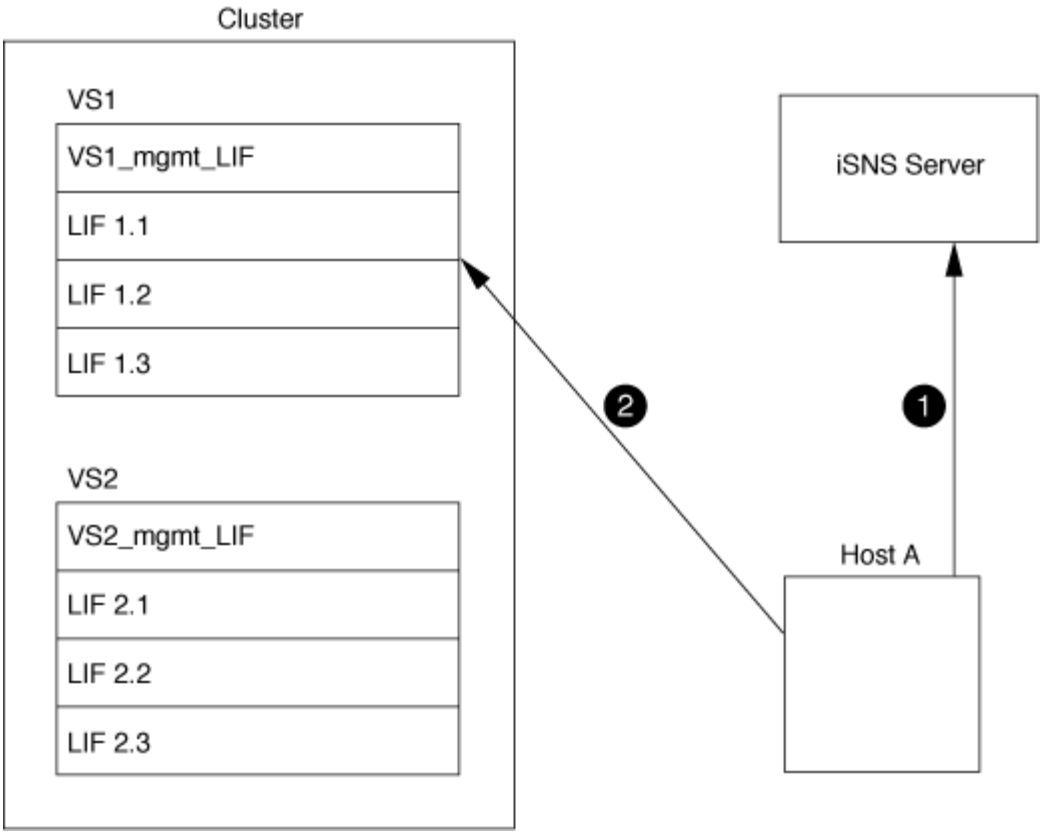
O servidor iSNS se comunica com cada máquina virtual de storage (SVM) por meio do LIF de gerenciamento do SVM. O LIF de gerenciamento Registra todos os nomes, alias e informações do portal do nó de destino iSCSI com o serviço iSNS para um SVM específico.

No exemplo a seguir, o SVM "'VS1'" usa o gerenciamento de SVM LIF "'VS1_mgmt_lif" para se Registrar no servidor iSNS. Durante o Registro do iSNS, um SVM envia todas as LIFs iSCSI por meio do LIF de gerenciamento do SVM para o iSNS Server. Depois que o Registro do iSNS for concluído, o servidor iSNS tem uma lista de todos os LIFs que servem iSCSI em "'VS1"". Se um cluster contiver vários SVMs, cada SVM

precisará se Registrar individualmente no servidor iSNS para usar o serviço iSNS.



No próximo exemplo, depois que o servidor iSNS concluir o Registro com o destino, o Host A pode descobrir todos os LIFs para "'VS1" através do servidor iSNS, conforme indicado na Etapa 1. Depois que o Host A concluir a descoberta dos LIFs para "'VS1"", o Host A pode estabelecer uma conexão com qualquer um dos LIFs em "'VS1"", como mostrado na Etapa 2. O host A não está ciente de nenhum dos LIFs em "'VS2" até que o LIF de gerenciamento "'VS2_mgmt_LIF" para Registros "'VS2" com o servidor iSNS.



No entanto, se você definir as listas de acesso à interface, o host só poderá usar as LIFs definidas na lista de acesso à interface para acessar o destino.

Depois que o iSNS for configurado inicialmente, o ONTAP atualizará automaticamente o servidor iSNS quando as configurações do SVM mudarem.

Pode ocorrer um atraso de alguns minutos entre o momento em que você faz as alterações de configuração e quando o ONTAP envia a atualização para o servidor iSNS. Forçar uma atualização imediata das informações do iSNS no servidor iSNS: `vserver iscsi isns update`

Comandos para gerenciar iSNS

O ONTAP fornece comandos para gerenciar seu serviço iSNS.

Se você quiser…	Use este comando…
Configurar um serviço iSNS	`vserver iscsi isns create`
Inicie um serviço iSNS	`vserver iscsi isns start`
Modifique um serviço iSNS	`vserver iscsi isns modify`
Exibir a configuração do serviço iSNS	`vserver iscsi isns show`
Forçar uma atualização das informações do iSNS registradas	`vserver iscsi isns update`

Pare um serviço iSNS	`vserver iscsi isns stop`
Remova um serviço iSNS	`vserver iscsi isns delete`
Veja a página de manual para um comando	`man command name`

Consulte a página de manual de cada comando para obter mais informações.

Provisionamento DE SAN com FC

Você deve estar ciente dos conceitos importantes que são necessários para entender como o ONTAP implementa uma SAN FC.

Como os nós de destino FC se conetam à rede

Os sistemas de storage e os hosts têm adaptadores para que possam ser conectados a switches FC com cabos.

Quando um nó é conetado à SAN FC, cada SVM Registra o World Wide Port Name (WWPN) de seu LIF com o switch Fabric Name Service. O WWNN do SVM e o WWPN de cada LIF é atribuído automaticamente pelo ONTAP.

> A conexão direta com nós de hosts com FC não é suportada, NPIV é necessária e isso requer que um switch seja usado. Com sessões iSCSI, a comunicação funciona com conexões roteadas ou conetadas diretamente à rede. No entanto, ambos os métodos são suportados com o ONTAP.

Como os nós FC são identificados

Cada SVM configurado com FC é identificado por um nome de nó mundial (WWNN).

Como WWPNs são usados

As WWPNs identificam cada LIF em uma SVM configurada para dar suporte ao FC. Essas LIFs utilizam as portas FC físicas em cada nó do cluster, que podem ser placas de destino FC, UTA ou UTA2 configuradas como FC ou FCoE nos nós.

- Criando um grupo de iniciadores

  Os WWPNs dos HBAs do host são usados para criar um grupo de iniciadores (iggroup). Um iggroup é usado para controlar o acesso do host a LUNs específicos. Você pode criar um grupo de iniciadores especificando uma coleção de WWPNs de iniciadores em uma rede FC. Quando você mapeia um LUN em um sistema de armazenamento para um grupo, você pode conceder a todos os iniciadores nesse grupo acesso a esse LUN. Se o WWPN de um host não estiver em um grupo que é mapeado para um LUN, esse host não terá acesso ao LUN. Isso significa que os LUNs não aparecem como discos nesse host.

  Você também pode criar conjuntos de portas para tornar um LUN visível apenas em portas de destino específicas. Um conjunto de portas consiste em um grupo de portas de destino FC. Você pode vincular um iggroup a um conjunto de portas. Qualquer host no grupo pode acessar os LUNs somente conetando-se às portas de destino no conjunto de portas.

- Identificação única de FC LIFs

  WWPNs identificam de forma exclusiva cada interface lógica FC. O sistema operacional host usa a combinação de WWNN e WWPN para identificar SVMs e FC LIFs. Alguns sistemas operacionais exigem vinculação persistente para garantir que o LUN seja exibido no mesmo ID de destino no host.

Como as atribuições de nomes em todo o mundo funcionam

Nomes mundiais são criados sequencialmente em ONTAP. No entanto, devido à forma como o ONTAP os atribui, eles podem parecer atribuídos em uma ordem não sequencial.

Cada adaptador tem um WWPN e WWNN pré-configurados, mas o ONTAP não usa esses valores pré-configurados. Em vez disso, o ONTAP atribui seus próprios WWPNs ou WWNNs, com base nos endereços MAC das portas Ethernet integradas.

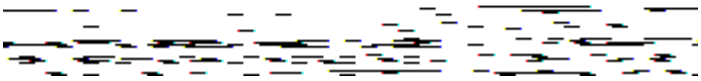
Os nomes mundiais podem parecer não sequenciais quando atribuídos pelas seguintes razões:

- Nomes mundiais são atribuídos em todos os nós e máquinas virtuais de storage (SVMs) no cluster.
- Os nomes do mundo livre são reciclados e adicionados de volta ao conjunto de nomes disponíveis.

Como os switches FC são identificados

Os switches Fibre Channel têm um nome de nó mundial (WWNN) para o próprio dispositivo e um nome de porta mundial (WWPN) para cada uma de suas portas.

Por exemplo, o diagrama a seguir mostra como os WWPNs são atribuídos a cada uma das portas em um switch Brocade de 16 portas. Para obter detalhes sobre como as portas são numeradas para um switch específico, consulte a documentação fornecida pelo fornecedor para esse switch.



Porta **0**, WWPN 20:**00**:00:60:69:51:06:B4

Porta **1**, WWPN 20:**01**:00:60:69:51:06:B4

Porta **14**, WWPN 20:**0e**:00:60:69:51:06:B4

Porta **15**, WWPN 20:**0f**:00:60:69:51:06:B4

Provisionamento DE SAN com NVMe

A partir do ONTAP 9.4, o NVMe/FC é compatível com ambiente SAN. O NVMe/FC permite que os administradores de storage provisionem namespaces e subsistemas e mapeem os namespaces para subsistemas, de forma semelhante à maneira como os LUNs são provisionados e mapeados para grupos de FC e iSCSI.

Um namespace NVMe é uma quantidade de memória não volátil que pode ser formatada em blocos lógicos. Namespaces são o equivalente a LUNs para protocolos FC e iSCSI, e um subsistema NVMe é análogo a um

iggroup. Um subsistema NVMe pode ser associado a iniciadores para que os namespaces dentro do subsistema possam ser acessados pelos iniciadores associados.

> Embora análogos em função, os namespaces NVMe não são compatíveis com todos os recursos compatíveis com LUNs.

A partir do ONTAP 9.5, é necessária uma licença para dar suporte ao acesso de dados voltado para o host com NVMe. Se o NVMe estiver habilitado no ONTAP 9.4, um período de carência de 90 dias será concedido para adquirir a licença após a atualização para o ONTAP 9.5. Se você tiver "ONTAP One", as licenças NVMe serão incluídas. Você pode ativar a licença usando o seguinte comando:

```
system license add -license-code NVMe_license_key
```

Informações relacionadas

"Relatório técnico da NetApp 4684: Implementando e configurando SANs modernas com NVMe/FC"

Volumes SAN

Sobre a visão geral dos volumes SAN

O ONTAP oferece três opções básicas de provisionamento de volume: Provisionamento thick, thin Provisioning e provisionamento semi-thick. Cada opção usa maneiras diferentes de gerenciar o espaço de volume e os requisitos de espaço para as tecnologias de compartilhamento de blocos do ONTAP. Entender como as opções funcionam permite que você escolha a melhor opção para o seu ambiente.

> Não é recomendável colocar LUNs SAN e compartilhamentos nas no mesmo FlexVol volume. Você deve provisionar volumes FlexVol separados, especificamente para suas LUNs de SAN, e provisionar volumes FlexVol separados, especificamente para seus compartilhamentos nas. Isso simplifica as implantações de gerenciamento e replicação, além de simplificar o modo como os volumes do FlexVol são suportados no Active IQ Unified Manager (anteriormente OnCommand Unified Manager).

Thin Provisioning para volumes

Quando um volume provisionado é criado, o ONTAP não reserva nenhum espaço extra quando o volume é criado. À medida que os dados são gravados no volume, o volume solicita o storage de que ele precisa do agregado para acomodar a operação de gravação. O uso de volumes provisionados por thin permite comprometer seu agregado, o que introduz a possibilidade de o volume não ser capaz de proteger o espaço necessário quando o agregado ficar sem espaço livre.

Você cria um FlexVol volume com provisionamento reduzido definindo sua `-space-guarantee` opção como `none`.

Provisionamento espesso para volumes

Quando um volume provisionado com espessura é criado, o ONTAP reserva armazenamento suficiente do agregado para garantir que qualquer bloco no volume possa ser gravado a qualquer momento. Ao configurar um volume para usar o provisionamento thick, você pode empregar qualquer um dos recursos de eficiência de storage da ONTAP, como compactação e deduplicação, para compensar os maiores requisitos de storage iniciais.

Você cria um FlexVol volume com provisionamento excessivo definindo sua `-space-slo` opção (objetivo de nível de serviço) como `thick`.

Provisionamento semi-espesso para volumes

Quando um volume usando provisionamento semi-espesso é criado, o ONTAP separa o espaço de armazenamento do agregado para contabilizar o tamanho do volume. Se o volume estiver sem espaço livre porque os blocos estão em uso por tecnologias de compartilhamento de bloco, o ONTAP se esforça para excluir objetos de dados de proteção (cópias Snapshot e arquivos FlexClone e LUNs) para liberar o espaço que eles estão segurando. Enquanto o ONTAP puder excluir os objetos de dados de proteção com a rapidez suficiente para acompanhar o espaço necessário para sobrescritas, as operações de gravação continuarão a ser bem-sucedidas. Isso é chamado de garantia de escrita "melhor esforço".

Observação: a seguinte funcionalidade não é suportada em volumes que usam provisionamento semi-espesso:

- tecnologias de eficiência de storage, como deduplicação, compressão e compactação
- Microsoft offloaded Data Transfer (ODX)

Você cria um FlexVol volume provisionado semi-espesso definindo sua `-space-slo` opção (objetivo de nível de serviço) como `semi-thick`.

Use com arquivos e LUNs reservados ao espaço

Um arquivo ou LUN com espaço reservado é aquele para o qual o armazenamento é alocado quando é criado. Historicamente, o NetApp usou o termo "LUN com provisionamento reduzido" para significar um LUN para o qual a reserva de espaço está desativada (um LUN sem espaço reservado).

*Nota: * Arquivos não reservados ao espaço não são geralmente chamados de "arquivos thin-provisionados".

A tabela a seguir resume as principais diferenças em como as três opções de provisionamento de volume podem ser usadas com arquivos reservados ao espaço e LUNs:

Provisionamento de volume	Reserva de espaço LUN/ficheiro	Sobrescreve	Proteção de dados 2	A eficiência de armazenamento 3
Espesso	Suportado	1	Garantido	Suportado
Fino	Sem efeito	Nenhum	Garantido	Suportado
Semi-espesso	Suportado	O melhor esforço 1	Melhor esforço	Não suportado

Notas

1. A capacidade de garantir substituições ou fornecer uma garantia de substituição de melhor esforço requer que a reserva de espaço esteja ativada no LUN ou arquivo.
2. Os dados de proteção incluem cópias Snapshot e arquivos FlexClone e LUNs marcados para exclusão automática (clones de backup).
3. A eficiência de storage inclui deduplicação, compactação, arquivos FlexClone e LUNs não marcados para exclusão automática (clones ativos) e subarquivos FlexClone (usados para descarregar cópias).

Suporte para LUNs de thin Provisioning SCSI

O ONTAP oferece suporte a T10 LUNs de thin Provisioning SCSI, bem como LUNs de thin Provisioning NetApp. O thin Provisioning SCSI T10 permite que os aplicativos host suportem recursos SCSI, incluindo recuperação de espaço LUN e recursos de monitoramento de espaço LUN para ambientes de blocos. O thin Provisioning SCSI T10 deve ser suportado pelo software de host SCSI.

Você usa a configuração ONTAP `space-allocation` para habilitar/desabilitar o suporte ao provisionamento de thin Provisioning T10 em um LUN. Você usa a configuração ONTAP `space-allocation enable` para habilitar o provisionamento de thin Provisioning SCSI T10 em um LUN.

O `[-space-allocation {enabled|disabled}]` comando no Manual de Referência de comando do ONTAP tem mais informações para habilitar/desabilitar o suporte ao provisionamento de thin Provisioning T10 e habilitar o provisionamento de thin Provisioning SCSI T10 em um LUN.

"Referência do comando ONTAP"

Configurar opções de provisionamento de volume

Você pode configurar um volume para thin Provisioning, thin Provisioning ou provisionamento semi-espesso.

Sobre esta tarefa

Definir a `-space-slo` opção para `thick` garantir o seguinte:

- Todo o volume é pré-alocado no agregado. Não é possível usar o `volume create` comando ou `volume modify` para configurar a opção do volume `-space-guarantee`.
- 100% do espaço necessário para as substituições é reservado. Você não pode usar o `volume modify` comando para configurar a opção do volume `-fractional-reserve`

Definir a `-space-slo` opção para `semi-thick` garantir o seguinte:

- Todo o volume é pré-alocado no agregado. Não é possível usar o `volume create` comando ou `volume modify` para configurar a opção do volume `-space-guarantee`.
- Nenhum espaço é reservado para substituições. Você pode usar o `volume modify` comando para configurar a opção do volume `-fractional-reserve`.
- A exclusão automática de cópias Snapshot está ativada.

Passo

1. Configurar opções de provisionamento de volume:

   `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-space-slo none|thick|semi-thick -space-guarantee none|volume`

   A `-space-guarantee` opção padrão é `none` para sistemas AFF e para volumes DP não AFF. Caso contrário, o padrão é `volume`. Para volumes FlexVol existentes, use o `volume modify` comando para configurar opções de provisionamento.

   O comando a seguir configura o vol1 no SVM VS1 para thin Provisioning:

```
cluster1::> volume create –vserver vs1 -volume vol1 -space-guarantee
none
```

O comando a seguir configura o vol1 no SVM VS1 para provisionamento espesso:

```
cluster1::> volume create –vserver vs1 -volume vol1 -space-slo thick
```

O comando a seguir configura o vol1 no SVM VS1 para provisionamento semi-espesso:

```
cluster1::> volume create –vserver vs1 -volume vol1 -space-slo semi-
thick
```

Opções de configuração de VOLUME SAN

Tem de definir várias opções no volume que contém o LUN. A forma como definir as opções de volume determina a quantidade de espaço disponível para LUNs no volume.

Crescimento automático

Você pode ativar ou desativar o crescimento automático. Se você ativá-lo, o crescimento automático permite que o ONTAP aumente automaticamente o tamanho do volume até um tamanho máximo que você predeterminar. Deve haver espaço disponível no agregado contendo para suportar o crescimento automático do volume. Portanto, se você ativar o crescimento automático, você deve monitorar o espaço livre no agregado contendo e adicionar mais quando necessário.

O crescimento automático não pode ser acionado para suportar a criação de Snapshot. Se você tentar criar uma cópia Snapshot e não houver espaço suficiente no volume, a criação de snapshot falhará, mesmo com o crescimento automático ativado.

Se o crescimento automático estiver desativado, o tamanho do seu volume permanecerá o mesmo.

Auto-retrátil

Pode ativar ou desativar o Autoshink. Se você ativá-lo, o recurso de auto-redução permite que o ONTAP diminua automaticamente o tamanho geral de um volume quando a quantidade de espaço consumida no volume diminui um limite predeterminado. Isso aumenta a eficiência de storage acionando volumes para liberar espaço livre não utilizado automaticamente.

snapshot Autodelete

O snapshot autodelete exclui automaticamente cópias snapshot quando uma das seguintes situações ocorre:

- O volume está quase cheio.
- O espaço de reserva do Snapshot está quase cheio.
- O espaço de reserva de substituição está cheio.

Você pode configurar o snapshot autodelete para excluir cópias Snapshot do mais antigo para o mais recente

ou do mais recente para o mais antigo. O snapshot autodelete não exclui cópias snapshot vinculadas a cópias snapshot em volumes clonados ou LUNs.

Se o seu volume precisar de espaço adicional e você tiver ativado o crescimento automático e o snapshot Autodelete, por padrão, o ONTAP tentará adquirir o espaço necessário acionando primeiro o crescimento automático. Se não for adquirido espaço suficiente através do crescimento automático, o snapshot autodelete é acionado.

Reserva do Snapshot

A reserva do Snapshot define a quantidade de espaço no volume reservado para cópias Snapshot. O espaço alocado à reserva Instantânea não pode ser usado para qualquer outra finalidade. Se todo o espaço alocado para o Snapshot Reserve for usado, as cópias Snapshot começarão a consumir espaço adicional no volume.

Requisito para movimentação de volumes em ambientes SAN

Antes de mover um volume que contenha LUNs ou namespaces, você precisa atender a certos requisitos.

- Para volumes que contêm um ou mais LUNs, você deve ter no mínimo dois caminhos por LUN (LIFs) conetados a cada nó no cluster.

  Isso elimina pontos únicos de falha e permite que o sistema sobreviva a falhas de componentes.

- Para volumes que contêm namespaces, o cluster precisa estar executando o ONTAP 9.6 ou posterior.

  A movimentação de volume não é compatível com configurações NVMe que executam o ONTAP 9.5.

Considerações para definir a reserva fracionária

A reserva fracionária, também chamada de *reserva de substituição LUN*, permite desativar a reserva de substituição para LUNs e arquivos reservados no espaço em um FlexVol volume. Isso pode ajudar a maximizar a utilização do storage, mas se o ambiente for afetado negativamente por falhas nas operações de gravação devido à falta de espaço, você precisa entender os requisitos que essa configuração impõe.

A configuração de reserva fracionária é expressa como uma porcentagem; os únicos valores válidos são `0` e `100` porcentagem. A configuração de reserva fracionária é um atributo do volume.

Definir a reserva fracionária para `0` aumentar a utilização do armazenamento. No entanto, um aplicativo que acessa dados que residem no volume pode ter uma interrupção de dados se o volume estiver sem espaço livre, mesmo com a garantia de volume definida como `volume`. No entanto, com a configuração e o uso adequados de volume, você pode minimizar a chance de falhas de gravação. O ONTAP fornece uma garantia de gravação "melhor esforço" para volumes com reserva fracionária definida para `0` quando *todos* dos seguintes requisitos são atendidos:

- A deduplicação não está em uso
- A compressão não está a ser utilizada
- Os subficheiros FlexClone não estão a ser utilizados
- Todos os arquivos FlexClone e LUNs FlexClone são ativados para exclusão automática

Esta não é a configuração padrão. Você deve ativar explicitamente a exclusão automática, seja no momento da criação ou modificando o arquivo FlexClone ou LUN FlexClone depois que ele for criado.

- A descarga de cópia ODX e FlexClone não está em uso
- A garantia de volume está definida para `volume`
- A reserva de espaço de arquivo ou LUN é `enabled`
- A reserva de instantâneo de volume está definida como `0`
- A exclusão automática da cópia Snapshot do volume é `enabled` com um nível de compromisso de `destroy`, uma lista de destruição de `lun_clone,vol_clone,cifs_share,file_clone,sfsr` e um gatilho de `volume`

  Essa configuração também garante que arquivos FlexClone e LUNs FlexClone sejam excluídos quando necessário.

Observe que, se sua taxa de alteração for alta, em casos raros, a exclusão automática da cópia Snapshot pode ficar para trás, resultando em falta de espaço no volume, mesmo com todas as configurações necessárias acima em uso.

Além disso, você pode, como opção, usar a funcionalidade de volume com crescimento automático para diminuir a probabilidade de as cópias do Snapshot precisarem ser excluídas automaticamente. Se você ativar a capacidade de crescimento automático, deverá monitorar o espaço livre no agregado associado. Se o agregado ficar cheio o suficiente para que o volume seja impedido de crescer, mais cópias Snapshot provavelmente serão excluídas à medida que o espaço livre no volume estiver esgotado.

Se você não puder atender a todos os requisitos de configuração acima e precisar garantir que o volume não fique sem espaço, defina a configuração de reserva fracionária do volume como `100`. Isso requer mais espaço livre na frente, mas garante que as operações de modificação de dados serão bem-sucedidas mesmo quando as tecnologias listadas acima estiverem em uso.

O valor padrão e os valores permitidos para a configuração de reserva fracionária dependem da garantia do volume:

Garantia de volume	Reserva fracionária predefinida	Valores permitidos
Volume	100	0, 100
Nenhum	0	0, 100

Gerenciamento de espaço no lado do host SAN

Em um ambiente com provisionamento reduzido, o gerenciamento de espaço no lado do host conclui o processo de gerenciamento de espaço do sistema de storage que foi liberado no sistema de arquivos do host.

Um sistema de arquivos host contém metadados para acompanhar quais blocos estão disponíveis para armazenar novos dados e quais blocos contêm dados válidos que não devem ser sobrescritos. Esses metadados são armazenados no LUN ou namespace. Quando um arquivo é excluído no sistema de arquivos host, os metadados do sistema de arquivos são atualizados para marcar os blocos desse arquivo como espaço livre. O espaço livre total do sistema de arquivos é então recalculado para incluir os blocos recém-liberados. Para o sistema de storage, essas atualizações de metadados não parecem diferentes de quaisquer

outras gravações que estejam sendo executadas pelo host. Portanto, o sistema de armazenamento não tem conhecimento de que quaisquer exclusões ocorreram.

Isso cria uma discrepância entre a quantidade de espaço livre relatada pelo host e a quantidade de espaço livre relatada pelo sistema de armazenamento subjacente. Por exemplo, suponha que você tenha um LUN de 200 GB recém-provisionado atribuído ao seu host pelo sistema de armazenamento. Tanto o host quanto o sistema de armazenamento relatam 200 GB de espaço livre. Seu host então grava 100 GB de dados. Nesse ponto, tanto o host quanto o sistema de armazenamento relatam 100 GB de espaço usado e 100 GB de espaço não utilizado.

Em seguida, você exclui 50 GB de dados do seu host. Neste ponto, seu host irá relatar 50 GB de espaço usado e 150 GB de espaço não utilizado. No entanto, seu sistema de armazenamento irá relatar 100 GB de espaço usado e 100 GB de espaço não utilizado.

O gerenciamento de espaço no lado do host usa vários métodos para reconciliar o diferencial de espaço entre o host e o sistema de armazenamento.

Gerenciamento de host simplificado com o SnapCenter

Você pode usar o software SnapCenter para simplificar algumas tarefas de gerenciamento e proteção de dados associadas ao storage iSCSI e FC. O SnapCenter é um pacote de gerenciamento opcional para hosts Windows e UNIX.

Você pode usar o software SnapCenter para criar facilmente discos virtuais de pools de storage que podem ser distribuídos entre vários sistemas de storage e automatizar as tarefas de provisionamento de storage e simplificar o processo de criação de cópias Snapshot e clones consistentes com os dados de host.

Consulte a documentação do produto NetApp para obter mais informações "SnapCenter" sobre .

Links relacionados

"Ativar a alocação de espaço ONTAP para protocolos SAN"

Sobre os grupos

Grupos de iniciadores (grupos de iniciadores) são tabelas de WWPNs de host de protocolo FC ou nomes de nós de host iSCSI. Você pode definir grupos e mapeá-los para LUNs para controlar quais iniciadores têm acesso a LUNs.

Normalmente, você deseja que todas as portas de iniciador do host ou iniciadores de software tenham acesso a um LUN. Se você estiver usando software multipathing ou tiver hosts em cluster, cada porta iniciador ou iniciador de software de cada host em cluster precisa de caminhos redundantes para o mesmo LUN.

Você pode criar grupos que especificam quais iniciadores têm acesso aos LUNs antes ou depois de criar LUNs, mas você deve criar grupos antes de poder mapear um LUN para um grupo.

Os grupos de iniciadores podem ter vários iniciadores, e vários grupos podem ter o mesmo iniciador. No entanto, não é possível mapear um LUN para vários grupos que tenham o mesmo iniciador. Um iniciador não pode ser um membro de grupos de diferentes ostypes.

Exemplo de como os grupos dão acesso LUN

Você pode criar vários grupos para definir quais LUNs estão disponíveis para seus hosts. Por exemplo, se você tiver um cluster de host, pode usar igroups para garantir que LUNs específicos sejam visíveis para apenas um host no cluster ou para todos os hosts no cluster.

A tabela a seguir ilustra como quatro grupos dão acesso aos LUNs para quatro hosts diferentes que estão acessando o sistema de armazenamento. Os hosts em cluster (Host3 e Host4) são membros do mesmo grupo (Group3) e podem acessar os LUNs mapeados para esse grupo. O grupo chamado Group4 contém as WWPNs de Host4 para armazenar informações locais que não se destinam a ser vistas por seu parceiro.

Hosts com WWPNs HBA, IQNs ou EUIs	grupos	WWPNs, IQNs, EUIs adicionados aos grupos	LUNs mapeados para grupos
Host1, caminho único (iniciador de software iSCSI) iqn.1991-05.com.microsoft:host1	group1	iqn.1991-05.com.microsoft:host1	`/vol/vol2/lun1`
Host2, multipath (dois HBAs) 10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	group2	10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	`/vol/vol2/lun2`
Host3, multipath, em cluster com host 4 10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02	group3	10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree1/lun3`
Host4, multipath, agrupado (não visível para Host3) 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	group4	10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree2/lun4` `/vol/vol2/qtree1/lun5`

Especifique WWPNs do iniciador e nomes de nó iSCSI para um grupo

Você pode especificar os nomes de nós iSCSI e WWPNs dos iniciadores quando você cria um iggroup ou pode adicioná-los mais tarde. Se você optar por especificar os nomes dos nós iSCSI do iniciador e WWPNs ao criar o LUN, eles poderão ser removidos mais tarde, se necessário.

Siga as instruções na documentação dos Utilitários de host para obter WWPNs e localizar os nomes de nó iSCSI associados a um host específico. Para hosts que executam o software ESX, use o Virtual Storage Console.

Virtualização de storage com descarga de cópia VMware e Microsoft

Visão geral da virtualização de storage com descarga de cópia VMware e Microsoft

VMware e Microsoft suportam operações de descarga de cópia para aumentar o desempenho e a taxa de transferência de rede. Você deve configurar o sistema para atender aos requisitos dos ambientes do sistema operacional VMware e Windows para usar suas respetivas funções de descarga de cópia.

Ao usar a descarga de cópia da VMware e da Microsoft em ambientes virtualizados, os LUNs precisam estar alinhados. LUNs desalinhados podem degradar o desempenho.

Vantagens de usar um ambiente SAN virtualizado

A criação de um ambiente virtualizado com o uso de máquinas virtuais de storage (SVMs) e LIFs permite expandir seu ambiente SAN para todos os nós do cluster.

- Gerenciamento distribuído

  É possível fazer login em qualquer nó da SVM para administrar todos os nós em um cluster.

- Maior acesso aos dados

  Com o MPIO e o ALUA, você tem acesso aos dados por meio de iSCSI ou FC LIFs ativos para o SVM.

- Acesso controlado LUN

  Se você usar SLM e portsets, poderá limitar quais LIFs um iniciador pode usar para acessar LUNs.

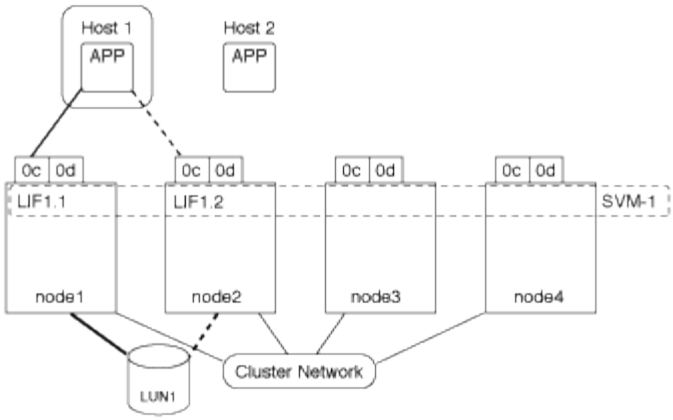
Como o acesso LUN funciona em um ambiente virtualizado

Em um ambiente virtualizado, os LIFs permitem que os hosts (clientes) acessem LUNs por meio de caminhos otimizados e não otimizados.

Um LIF é uma interface lógica que coneta o SVM a uma porta física. Embora vários SVMs possam ter várias LIFs na mesma porta, um LIF pertence a uma SVM. Você pode acessar LUNs por meio das LIFs SVMs.

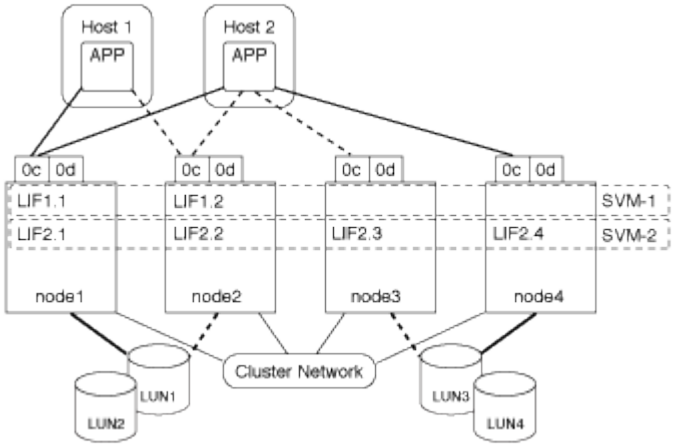
Exemplo de acesso LUN com uma única SVM em um cluster

No exemplo a seguir, o host 1 se conecta ao LIF1,1 e LIF1,2 no SVM-1 para acessar o LUN1. LIF1,1 usa a porta física node1:0C e LIF1,2 usa o node2:0C. O LIF1,1 e o LIF1,2 pertencem apenas à SVM-1. Se um novo LUN for criado no nó 1 ou no nó 2, para SVM-1, ele poderá usar essas mesmas LIFs. Se um novo SVM for criado, novas LIFs poderão ser criadas usando as portas físicas 0C ou 0d em ambos os nós.



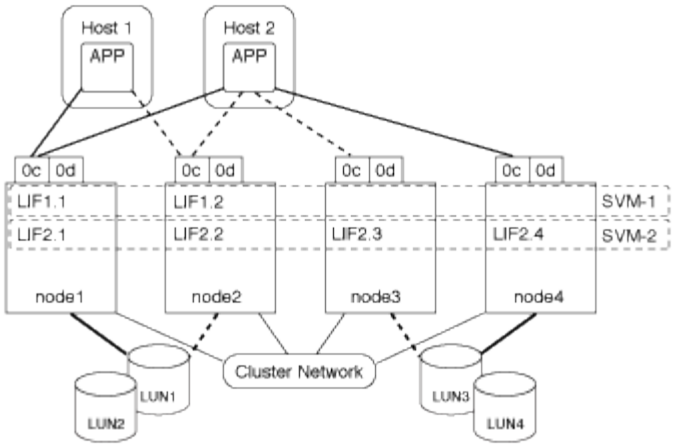
Exemplo de acesso LUN com vários SVMs em um cluster

Uma porta física pode suportar vários LIFs que servem diferentes SVMs. Como os LIFs estão associados a uma SVM específica, os nós de cluster podem enviar o tráfego de dados de entrada para o SVM correto. No exemplo a seguir, cada nó de 1 a 4 tem um LIF para SVM-2 usando a porta física 0C em cada nó. O host 1 se conecta ao LIF1,1 e ao LIF1,2 na SVM-1 para acessar o LUN1. O host 2 se conecta ao LIF2-1 e ao LIF2-2 na SVM-2 para acessar o LUN2. Ambos os SVMs estão compartilhando a porta física 0C nos nós 1 e 2. O SVM-2 tem LIFs adicionais que o host 2 está usando para acessar LUNs 3 e 4. Esses LIFs estão usando a porta física 0C nos nós 3 e 4. Vários SVMs podem compartilhar as portas físicas nos nós.



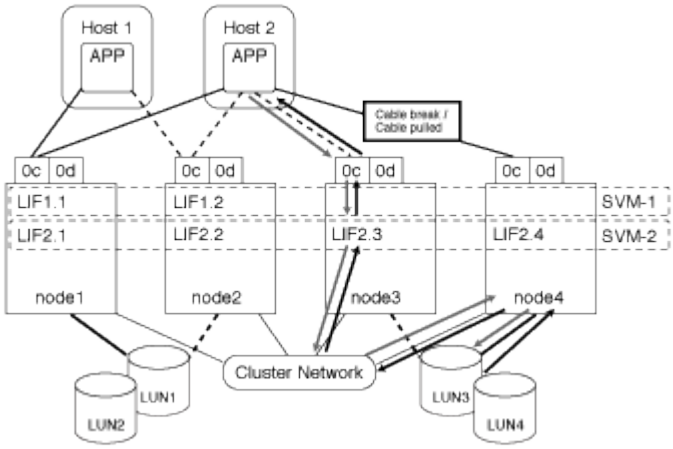
Exemplo de um caminho ativo ou otimizado para um LUN a partir de um sistema host

Em um caminho ativo ou otimizado, o tráfego de dados não percorre a rede do cluster; ele viaja a rota mais direta para o LUN. O caminho ativo ou otimizado para LUN1 é através de LIF1,1 em node1, usando a porta física 0C. O host 2 tem dois caminhos ativos ou otimizados, um caminho para node1, LIF2,1, que está compartilhando a porta física 0C e o outro caminho para node4, LIF2,4, que está usando a porta física 0C.



Exemplo de um caminho ativo ou não otimizado (indireto) para um LUN a partir de um sistema host

Em um caminho ativo ou não otimizado (indireto), o tráfego de dados viaja pela rede do cluster. Esse problema ocorre somente se todos os caminhos ativos ou otimizados de um host não estiverem disponíveis para lidar com o tráfego. Se o caminho do Host 2 para o SVM-2 LIF2,4 for perdido, o acesso ao LUN3 e ao LUN4 percorre a rede do cluster. O acesso a partir do Host 2 usa o LIF2,3 em node3. Em seguida, o tráfego entra no switch de rede do cluster e faz backup de até node4 para acesso ao LUN3 e ao LUN4. Em seguida, ele passará para trás pelo switch de rede de cluster e, em seguida, voltará para o LIF2,3 para o Host 2. Esse caminho ativo ou não otimizado é usado até que o caminho para o LIF2,4 seja restaurado ou um novo LIF seja estabelecido para SVM-2 em outra porta física no nó 4.



=
:allow-uri-read:

Melhorar o desempenho do VMware VAAI para hosts ESX

O ONTAP oferece suporte a determinados recursos de VMware vStorage APIs para integração de storage (VAAI) quando o host ESX estiver executando o ESX 4,1 ou posterior. Esses recursos ajudam a descarregar as operações do host ESX para o sistema de storage e a aumentar a taxa de transferência da rede. O host ESX habilita os recursos automaticamente no ambiente correto.

O recurso VAAI suporta os seguintes comandos SCSI:

- `EXTENDED_COPY`

Esse recurso permite que o host inicie a transferência de dados entre os LUNs ou em um LUN sem envolver o host na transferência de dados. Isso resulta em salvar ciclos de CPU ESX e aumentar a taxa de transferência da rede. O recurso de cópia estendida, também conhecido como "descarga de cópia", é usado em cenários como clonagem de uma máquina virtual. Quando invocado pelo host ESX, o recurso de descarga de cópia copia os dados dentro do sistema de storage em vez de passar pela rede do host. A descarga de cópia transfere dados das seguintes maneiras:

  - Dentro de um LUN
  - Entre LUNs em um volume
  - Entre LUNs em diferentes volumes em uma máquina virtual de storage (SVM)
  - Entre LUNs em diferentes SVMs dentro de um cluster se esse recurso não puder ser invocado, o host ESX usa automaticamente os comandos padrão DE LEITURA e GRAVAÇÃO para a operação de cópia.

- `WRITE_SAME`

  Esse recurso descarrega o trabalho de escrever um padrão repetido, como todos os zeros, para um storage array. O host ESX usa esse recurso em operações como o preenchimento zero de um arquivo.

- `COMPARE_AND_WRITE`

  Esse recurso ignora certos limites de simultaneidade de acesso a arquivos, o que acelera operações como inicializar máquinas virtuais.

Requisitos para usar o ambiente VAAI

Os recursos VAAI fazem parte do sistema operacional ESX e são invocados automaticamente pelo host ESX quando você configurou o ambiente correto.

Os requisitos ambientais são os seguintes:

- O host ESX deve estar executando o ESX 4,1 ou posterior.
- O sistema de storage NetApp que hospeda o armazenamento de dados VMware deve estar executando o ONTAP.
- (Somente descarga de cópia) a origem e o destino da operação de cópia VMware devem ser hospedados no mesmo sistema de storage no mesmo cluster.

> O recurso de descarga de cópia atualmente não oferece suporte à cópia de dados entre datastores VMware hospedados em diferentes sistemas de storage.

Determine se os recursos VAAI são suportados pelo ESX

Para confirmar se o sistema operacional ESX suporta os recursos VAAI, você pode verificar o vSphere Client ou usar qualquer outro meio de acessar o host. O ONTAP suporta os comandos SCSI por padrão.

Você pode verificar as configurações avançadas do host ESX para determinar se os recursos do VAAI estão ativados. A tabela indica quais comandos SCSI correspondem aos nomes de controle ESX.

Comando SCSI	Nome do controle ESX (recurso VAAI)
EXTENDED_COPY (CÓPIA_ESTENDIDA)	`HardwareAcceleratedMove`
WRITE_SAME	`HardwareAcceleratedInit`
COMPARE_E_ESCREVA	`HardwareAcceleratedLocking`

Microsoft offloaded Data Transfer (ODX)

A Microsoft Offloaded Data Transfer (ODX), também conhecida como *copy offload*, permite transferências diretas de dados dentro de um dispositivo de armazenamento ou entre dispositivos de armazenamento compatíveis sem transferir os dados através do computador host.

O ONTAP oferece suporte ao ODX para os protocolos SMB e SAN.

Em transferências de arquivos não ODX, os dados são lidos da origem e são transferidos pela rede para o host. O host transfere os dados de volta pela rede para o destino. Na transferência de arquivos ODX, os dados são copiados diretamente da origem para o destino sem passar pelo host.

Como as cópias descarregadas do ODX são executadas diretamente entre a origem e o destino, benefícios significativos de desempenho são obtidos se as cópias forem executadas dentro do mesmo volume, incluindo tempo de cópia mais rápido para cópias do mesmo volume, utilização reduzida da CPU e memória no cliente e utilização reduzida da largura de banda de e/S de rede. Se as cópias estiverem em volumes, talvez não haja ganhos significativos de desempenho em comparação com as cópias baseadas em host.

Para ambientes SAN, o ODX só está disponível quando é suportado pelo host e pelo sistema de armazenamento. Os computadores clientes que suportam ODX e têm o ODX ativado automaticamente e de forma transparente usam transferência de arquivos descarregados ao mover ou copiar arquivos. O ODX é usado independentemente de você arrastar e soltar arquivos através do Windows Explorer ou usar comandos de cópia de arquivo de linha de comando ou se um aplicativo cliente inicia solicitações de cópia de arquivo.

Requisitos para usar ODX

Se você planeja usar o ODX para descarregamentos de cópias, você precisa estar familiarizado com considerações de suporte de volume, requisitos de sistema e requisitos de capacidade de software.

Para usar o ODX, seu sistema deve ter o seguinte:

- ONTAP

  O ODX é ativado automaticamente em versões suportadas do ONTAP.

- Volume mínimo de origem de 2 GB

  Para um desempenho ideal, o volume de origem deve ser superior a 260 GB.

- Suporte ODX no cliente Windows

  O ODX é suportado no Windows Server 2012 ou posterior e no Windows 8 ou posterior. A Matriz de interoperabilidade contém as informações mais recentes sobre clientes Windows suportados.

"Ferramenta de Matriz de interoperabilidade do NetApp"

- Cópia de suporte de aplicativo para ODX

  O aplicativo que executa a transferência de dados deve suportar ODX. As operações de aplicação que suportam ODX incluem o seguinte:

  - Operações de gerenciamento do Hyper-V, como criar e converter discos rígidos virtuais (VHDs), gerenciar cópias Snapshot e copiar arquivos entre máquinas virtuais
  - Operações do Windows Explorer
  - Comandos de cópia do Windows PowerShell
  - Comandos de cópia do prompt de comando do Windows a Biblioteca Microsoft TechNet contém mais informações sobre aplicativos ODX suportados em servidores e clientes Windows.
- Se você usar volumes compatados, o tamanho do grupo de compactação deve ser 8K.

  O tamanho do grupo de compressão 32K não é suportado.

O ODX não funciona com os seguintes tipos de volume:

- Volumes de origem com capacidades inferiores a 2 GB
- Volumes só de leitura
- "Volumes FlexCache"

  O ODX é compatível com volumes de origem FlexCache.
- "Volumes provisionados semi-grossos"

Requisitos especiais de arquivo do sistema

Você pode excluir arquivos ODX encontrados no qtrees. Não remova ou modifique quaisquer outros arquivos de sistema ODX, a menos que você seja informado pelo suporte técnico para fazê-lo.

Ao usar o recurso ODX, existem arquivos de sistema ODX que existem em cada volume do sistema. Esses arquivos permitem a representação pontual dos dados usados durante a transferência do ODX. Os seguintes arquivos de sistema estão no nível raiz de cada volume que contém LUNs ou arquivos para os quais os dados foram descarregados:

- `.copy-offload` (um diretório oculto)
- `.tokens` (arquivo sob o diretório oculto `.copy-offload`)

Você pode usar o `copy-offload delete-tokens -path dir_path -node` *`node_name`* comando para excluir uma qtree contendo um arquivo ODX.

Casos de uso para ODX

Você deve estar ciente dos casos de uso para usar o ODX em SVMs para que você possa determinar em que circunstâncias o ODX fornece benefícios de desempenho.

Os servidores e clientes do Windows que suportam ODX usam a descarga de cópia como a forma padrão de copiar dados em servidores remotos. Se o servidor ou cliente do Windows não suportar ODX ou a descarga de cópia ODX falhar em qualquer ponto, a operação de cópia ou movimentação volta para leituras e

gravações tradicionais para a operação de cópia ou movimentação.

Os seguintes casos de uso suportam o uso de cópias e movimentos ODX:

- Intra-volume

  Os arquivos de origem e destino ou LUNs estão dentro do mesmo volume.

- Entre volumes, mesmo nó e SVM

  Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem ao mesmo SVM.

- Entre volumes, nós diferentes e o mesmo SVM

  Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem ao mesmo SVM.

- Entre SVM, mesmo nó

  O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem a diferentes SVMs.

- Entre SVM, nós diferentes

  O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem a diferentes SVMs.

- Inter-cluster

  As LUNs de origem e destino estão em volumes diferentes, localizados em nós diferentes, entre clusters. Isso só é suportado para SAN e não funciona para SMB.

Existem alguns casos de uso especiais adicionais:

- Com a implementação do ONTAP ODX, você pode usar o ODX para copiar arquivos entre compartilhamentos SMB e unidades virtuais conetadas a FC ou iSCSI.

  Você pode usar o Windows Explorer, a CLI do Windows ou PowerShell, Hyper-V ou outras aplicações compatíveis com ODX para copiar ou mover arquivos sem interrupções usando a descarga de cópia ODX entre compartilhamentos SMB e LUNs conetados, desde que os compartilhamentos SMB e LUNs estejam no mesmo cluster.

- O Hyper-V fornece alguns casos de uso adicionais para descarga de cópia ODX:

  - Você pode usar a passagem de descarga de cópia ODX com o Hyper-V para copiar dados dentro ou através de arquivos de disco rígido virtual (VHD) ou para copiar dados entre compartilhamentos SMB mapeados e LUNs iSCSI conetados dentro do mesmo cluster.

    Isso permite que cópias de sistemas operacionais convidados passem para o storage subjacente.

  - Ao criar VHDs de tamanho fixo, o ODX é usado para inicializar o disco com zeros, usando um token zerado bem conhecido.
  - A descarga de cópia ODX é usada para migração de armazenamento de máquina virtual se o armazenamento de origem e destino estiver no mesmo cluster.

Para aproveitar os casos de uso para a passagem de descarga de cópia ODX com Hyper-V, o sistema operacional convidado deve suportar ODX e os discos do sistema operacional convidado devem ser discos SCSI suportados pelo armazenamento (SMB ou SAN) que suporte ODX. Os discos IDE no sistema operacional convidado não suportam passagem ODX.

Administração da SAN

Provisionamento DE SAN

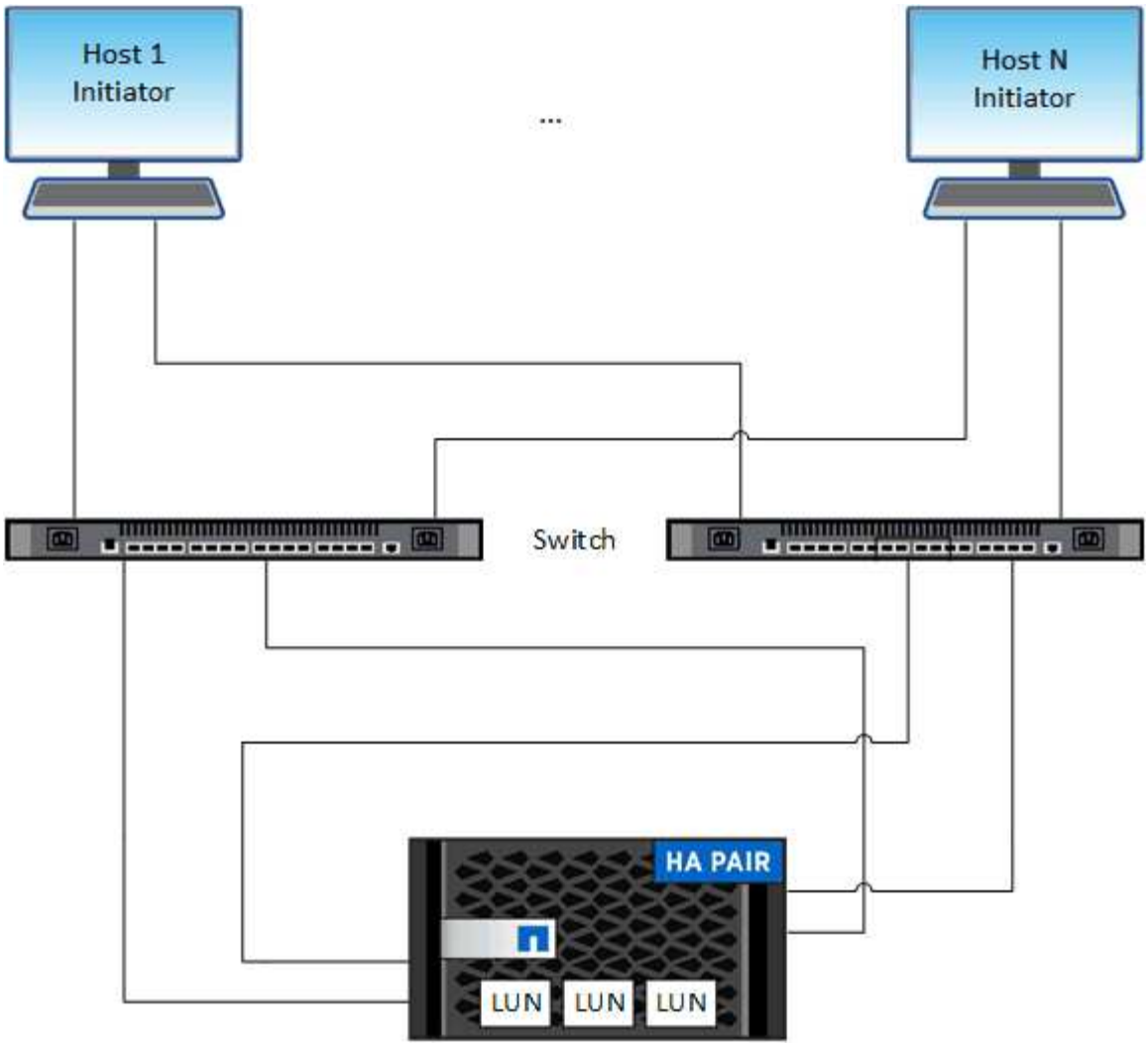
Visão geral do gerenciamento DE SAN

O conteúdo desta seção mostra como configurar e gerenciar ambientes SAN com a interface de linha de comando (CLI) do ONTAP e o Gerenciador de sistemas no ONTAP 9.7 e versões posteriores.

Se você estiver usando o gerenciador de sistema clássico (disponível somente no ONTAP 9.7 e versões anteriores), consulte estes tópicos:

- "Protocolo iSCSI"
- "Protocolo FC/FCoE"

Você pode usar os protocolos iSCSI e FC para fornecer storage em um ambiente SAN.



Com iSCSI e FC, os destinos de armazenamento são chamados de LUNs (unidades lógicas) e são apresentados aos hosts como dispositivos de bloco padrão. Você cria LUNs e, em seguida, mapeia-os para grupos de iniciadores (grupos de iniciadores). Grupos de iniciadores são tabelas de WWPs de host FC e nomes de nós de host iSCSI e controlam quais iniciadores têm acesso a quais LUNs.

Os destinos FC se conetam à rede por meio de switches FC e adaptadores do lado do host e são identificados por nomes de portas mundiais (WWPNs). Os destinos iSCSI se conetam à rede por meio de adaptadores de rede Ethernet (NICs) padrão, placas de mecanismo de descarga TCP (TOE) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host dedicados (HBAs) e são identificados por nomes qualificados iSCSI (IQNs).

Para mais informações

Se você tiver um sistema de storage ASA R2 (ASA A1K, ASA A70, ASA A90), consulte "Documentação do sistema de storage ASA R2".

Configurar switches para FCoE

Você deve configurar seus switches para FCoE antes que seu serviço FC possa ser executado sobre a infraestrutura Ethernet existente.

O que você vai precisar

- Sua configuração SAN precisa ser compatível.

Para obter mais informações sobre as configurações suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

- Um adaptador de destino unificado (UTA) deve ser instalado em seu sistema de armazenamento.

  Se você estiver usando um UTA2, ele deve ser definido para `cna` o modo.

- Um adaptador de rede convergente (CNA) deve ser instalado em seu host.

Passos

1. Use a documentação do switch para configurar os switches para FCoE.
2. Verifique se as configurações do DCB para cada nó no cluster foram configuradas corretamente.

   ```
   run -node node1 -command dcb show
   ```

   As definições do DCB são configuradas no interrutor. Consulte a documentação do switch se as configurações estiverem incorretas.

3. Verifique se o login FCoE está funcionando quando o status on-line da porta de destino FC for `true`.

   ```
   fcp adapter show -fields node,adapter,status,state,speed,fabric-
   established,physical-protocol
   ```

   Se o status on-line da porta de destino FC for `false`, consulte a documentação do switch.

Informações relacionadas

- "Ferramenta de Matriz de interoperabilidade do NetApp"
- "Relatório técnico da NetApp 3800: Guia de implantação completa em Fibre Channel over Ethernet (FCoE)"
- "Guias de configuração de software Cisco MDS 9000 NX-os e SAN-os"
- "Produtos Brocade"

Requisitos do sistema

A configuração de LUNs envolve a criação de um LUN, a criação de um grupo e o mapeamento do LUN para o grupo. O sistema deve atender a certos pré-requisitos antes de configurar os LUNs.

- A Matriz de interoperabilidade deve listar sua configuração de SAN como suportada.
- Seu ambiente SAN precisa atender aos limites de configuração de controladora e host SAN especificados na "NetApp Hardware Universe" para sua versão do software ONTAP.
- É necessário instalar uma versão suportada dos Utilitários do sistema anfitrião.

  A documentação Host Utilities (Utilitários do host) fornece mais informações.

- Você precisa ter SAN LIFs no nó proprietário do LUN e no parceiro de HA do nó proprietário.

Informações relacionadas

- "Ferramenta de Matriz de interoperabilidade do NetApp"
- "Configuração do host SAN ONTAP"
- "Relatório técnico da NetApp 4017: Práticas recomendadas de SAN Fibre Channel"

O que saber antes de criar um LUN

Por que os tamanhos reais de LUN variam ligeiramente

Você deve estar ciente do seguinte em relação ao tamanho de seus LUNs.

- Quando você cria um LUN , o tamanho real do LUN pode variar ligeiramente com base no tipo de SO do LUN. O tipo de SO LUN não pode ser modificado após a criação do LUN.
- Se você criar um LUN no tamanho máximo de LUN, esteja ciente de que o tamanho real do LUN pode ser um pouco menor. ONTAP arredonda o limite para ser um pouco menos.
- Os metadados para cada LUN requerem aproximadamente 64 KB de espaço no agregado que contém. Ao criar um LUN, você deve garantir que o agregado que contém tenha espaço suficiente para os metadados do LUN. Se o agregado não contiver espaço suficiente para os metadados do LUN, alguns hosts poderão não conseguir acessar o LUN.

Diretrizes para a atribuição de IDs de LUN

Normalmente, o ID de LUN padrão começa com 0 e é atribuído em incrementos de 1 para cada LUN mapeado adicional. O host associa a ID LUN com o local e o nome do caminho do LUN. O intervalo de números de ID LUN válidos depende do host. Para obter informações detalhadas, consulte a documentação fornecida com seus Utilitários de host.

Diretrizes para mapeamento de LUNs para grupos

- Você pode mapear um LUN apenas uma vez para um grupo.
- Como prática recomendada, você deve mapear um LUN para apenas um iniciador específico através do grupo.
- Você pode adicionar um único iniciador a vários grupos, mas o iniciador pode ser mapeado para apenas um LUN.
- Não é possível usar o mesmo ID de LUN para dois LUNs mapeados para o mesmo grupo.
- Você deve usar o mesmo tipo de protocolo para grupos e conjuntos de portas.

Verifique e adicione sua licença de protocolo FC ou iSCSI

Antes de habilitar o acesso a bloco de uma máquina virtual de storage (SVM) com FC ou iSCSI, você precisa ter uma licença. As licenças FC e iSCSI estão incluídas no "ONTAP One".

Exemplo 1. Passos

System Manager

Se você não tiver o ONTAP One, verifique e adicione sua licença FC ou iSCSI com o Gerenciador de sistema do ONTAP (9,7 e posterior).

1. No System Manager, selecione **Cluster > Settings > Licenses**
2. Se a licença não estiver listada, + Add selecione e insira a chave de licença.
3. Selecione **Adicionar**.

CLI

Se você não tiver o ONTAP One, verifique e adicione sua licença FC ou iSCSI com a CLI do ONTAP.

1. Verifique se você tem uma licença ativa para FC ou iSCSI.

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- --------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. Se não tiver uma licença ativa para FC ou iSCSI, adicione o seu código de licença.

```
license add -license-code <your_license_code>
```

Provisionamento de storage SAN

Esse procedimento cria novos LUNs em uma VM de storage existente que já tenha o protocolo FC ou iSCSI configurado.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para provisionar seu storage. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Se for necessário criar uma nova VM de storage e configurar o protocolo FC ou iSCSI, consulte "Configurar um SVM para FC" ou "Configurar um SVM para iSCSI".

Se a licença FC não estiver ativada, os LIFs e SVMs parecem estar online, mas o status operacional está

inativo.

Os LUNs aparecem no seu host como dispositivos de disco.

> O acesso de unidade lógica assimétrica (ALUA) é sempre ativado durante a criação de LUN. Não é possível alterar a definição ALUA.

Você deve usar o zoneamento de iniciador único para todos os LIFs FC no SVM para hospedar os iniciadores.

A partir do ONTAP 9.8, quando você provisiona o storage, a QoS é habilitada por padrão. Você pode desativar o QoS ou escolher uma política de QoS personalizada durante o processo de provisionamento ou posteriormente.

Exemplo 2. Passos

System Manager

Criar LUNs para fornecer storage para um host SAN usando o protocolo FC ou iSCSI com o Gerenciador de sistemas ONTAP (9,7 e posterior).

Para concluir esta tarefa utilizando o System Manager Classic (disponível com 9,7 e anterior), consulte "Configuração iSCSI para Red Hat Enterprise Linux"

Passos

1. Instale o apropriado "Utilitários de host SAN" em seu host.
2. No System Manager, clique em **Storage > LUNs** e, em seguida, clique em **Add**.
3. Introduza as informações necessárias para criar o LUN.
4. Você pode clicar em **mais Opções** para fazer qualquer uma das seguintes opções, dependendo da sua versão do ONTAP.

Opção	Disponível a partir de
• Atribuir política de QoS a LUNs em vez de volume pai ◦ **Mais Opções > armazenamento e Otimização** ◦ Selecione **nível de serviço de desempenho**. ◦ Para aplicar a política de QoS a LUNs individuais em vez de todo o volume, selecione **aplicar esses limites de desempenho a cada LUN**. Por padrão, os limites de desempenho são aplicados ao nível do volume.	ONTAP 9.10,1
• Crie um novo grupo de iniciadores usando grupos de iniciadores existentes ◦ **Mais Opções > INFORMAÇÕES DO HOST** ◦ Selecione **novo grupo de iniciadores usando grupos de iniciadores existentes**. ⓘ O tipo de sistema operacional para um grupo contendo outros grupos não pode ser alterado depois que ele foi criado.	ONTAP 9.9,1
• Adicione uma descrição ao seu grupo ou iniciador do host A descrição serve como um alias para o igroup ou iniciador do host. ◦ **Mais Opções > INFORMAÇÕES DO HOST**	ONTAP 9.9,1

• Crie seu LUN em um volume existente Por padrão, um novo LUN é criado em um novo volume. ◦ **Mais Opções > Adicionar LUNs** ◦ Selecione **Group Related LUNs**.	ONTAP 9.9,1
• Desative a QoS ou escolha uma política de QoS personalizada ◦ **Mais Opções > armazenamento e Otimização** ◦ Selecione **nível de serviço de desempenho**. No ONTAP 9.9,1 e posterior, se você selecionar uma política de QoS personalizada, também poderá selecionar posicionamento manual em um nível local especificado.	ONTAP 9,8

5. Para FC, coloque a zona dos seus comutadores FC pela WWPN. Use uma zona por iniciador e inclua todas as portas de destino em cada zona.
6. Descubra LUNs no seu host.

   Para o VMware vSphere, use o Virtual Storage Console (VSC) para descobrir e inicializar seus LUNs.
7. Inicialize os LUNs e, opcionalmente, crie sistemas de arquivos.
8. Verifique se o host pode gravar e ler dados no LUN.

CLI

Crie LUNs para fornecer storage para um host SAN usando o protocolo FC ou iSCSI com a CLI do ONTAP.

1. Verifique se você tem uma licença para FC ou iSCSI.

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. Se você não tiver uma licença para FC ou iSCSI, use o `license add` comando.

```
license add -license-code <your_license_code>
```

3. Habilite o serviço de protocolos no SVM:

   Para iSCSI:

   ```
   vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
   ```

   Para FC:

   ```
   vserver fcp create -vserver <svm_name> -status-admin up
   ```

4. Crie duas LIFs para as SVMs em cada nó:

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -role
   data -data-protocol <iscsi|fc> -home-node <node_name> -home-port
   <port_name> -address <ip_address> -netmask <netmask>
   ```

   O NetApp é compatível com, no mínimo, um iSCSI ou FC LIF por nó para cada SVM que fornece dados. No entanto, dois LIFS por nó são necessários para redundância. Para iSCSI, é recomendável configurar um mínimo de duas LIFs por nó em redes Ethernet separadas.

5. Verifique se seus LIFs foram criados e se o status operacional deles é `online`:

   ```
   network interface show -vserver <svm_name> <lif_name>
   ```

6. Crie seus LUNs:

   ```
   lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>
   -size <lun_size> -ostype linux -space-reserve <enabled|disabled>
   ```

   O seu nome LUN não pode exceder 255 carateres e não pode conter espaços.

   ⓘ A opção NVFAIL é ativada automaticamente quando um LUN é criado em um volume.

7. Crie seus grupos:

   ```
   igroup create -vserver <svm_name> -igroup <igroup_name> -protocol
   <fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
   ```

8. Mapeie seus LUNs para grupos:

```
lun mapping create -vserver <svm_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. Verifique se os LUNs estão configurados corretamente:

```
lun show -vserver <svm_name>
```

10. Opcionalmente"Crie um conjunto de portas e vincule a um grupo", .
11. Siga as etapas na documentação do host para habilitar o acesso a blocos em seus hosts específicos.
12. Use os Utilitários do host para concluir o mapeamento FC ou iSCSI e descobrir os LUNs no host.

Informações relacionadas

- "Visão geral da administração DE SAN"
- "Configuração do host SAN ONTAP"
- "Exibir e gerenciar grupos de iniciadores SAN no System Manager"
- "Relatório técnico da NetApp 4017: Práticas recomendadas de SAN Fibre Channel"

Provisionamento NVMe

Visão geral do NVMe

Você pode usar o protocolo NVMe (non-volátil Memory Express) para fornecer storage em um ambiente SAN. O protocolo NVMe é otimizado para performance com storage de estado sólido.

Para NVMe, os destinos de storage são chamados de namespaces. Um namespace NVMe é uma quantidade de storage não volátil que pode ser formatada em blocos lógicos e apresentada a um host como um dispositivo de bloco padrão. Você cria namespaces e subsistemas e, em seguida, mapeia os namespaces para os subsistemas, semelhante à maneira como os LUNs são provisionados e mapeados para grupos para FC e iSCSI.

Os destinos NVMe são conectados à rede por meio de uma infraestrutura FC padrão usando switches FC ou uma infraestrutura TCP padrão usando switches Ethernet e adaptadores no lado do host.

O suporte a NVMe varia de acordo com a sua versão do ONTAP. "Limitações e suporte do NVMe"Consulte para obter detalhes.

O que é NVMe

O protocolo não volátil Memory Express (NVMe) é um protocolo de transporte usado para acessar Mídia de storage não volátil.

O NVMe sobre Fabrics (NVMeoF) é uma extensão definida por especificação do NVMe que permite a comunicação baseada em NVMe por conexões que não PCIe. Esta interface permite que gabinetes de armazenamento externos sejam conetados a um servidor.

O NVMe foi desenvolvido para fornecer acesso eficiente a dispositivos de storage criados com memória não

volátil, da tecnologia flash às tecnologias de memória persistente e de alta performance. Como tal, ele não tem as mesmas limitações que os protocolos de armazenamento projetados para unidades de disco rígido. Os dispositivos flash e de estado sólido (SSDs) são um tipo de memória não volátil (NVM). NVM é um tipo de memória que mantém seu conteúdo durante uma queda de energia. O NVMe é uma maneira de acessar essa memória.

Os benefícios do NVMe incluem maiores velocidades, produtividade, taxa de transferência e capacidade para transferência de dados. As caraterísticas específicas incluem o seguinte:

- O NVMe foi projetado para ter até 64 mil filas.

  Cada fila, por sua vez, pode ter até 64 mil comandos simultâneos.

- O NVMe é compatível com vários fornecedores de hardware e software
- O NMVe é mais produtivo com as tecnologias Flash que permitem tempos de resposta mais rápidos
- O NVMe permite várias solicitações de dados para cada "demanda" enviada para o SSD.

  O NVMe leva menos tempo para decodificar um "request" e não requer bloqueio de threads em um programa multithread.

- O NVMe oferece suporte a funcionalidades que impedem a perda de peso no nível da CPU e permitem escalabilidade massiva à medida que os sistemas se expandem.

Sobre os namespaces NVMe

Um namespace NVMe é uma quantidade de memória não volátil (NVM) que pode ser formatada em blocos lógicos. Namespaces são usados quando uma máquina virtual de storage é configurada com o protocolo NVMe e são equivalentes a LUNs para protocolos FC e iSCSI.

Um ou mais namespaces são provisionados e conectados a um host NVMe. Cada namespace pode suportar vários tamanhos de bloco.

O protocolo NVMe fornece acesso a namespaces por meio de várias controladoras. Usando drivers NVMe, que são compatíveis com a maioria dos sistemas operacionais, os namespaces de unidade de estado sólido (SSD) aparecem como dispositivos de bloco padrão nos quais sistemas de arquivos e aplicativos podem ser implantados sem qualquer modificação.

Um ID de namespace (NSID) é um identificador usado por um controlador para fornecer acesso a um namespace. Ao definir o NSID para um host ou grupo de hosts, você também configura a acessibilidade a um volume por um host. Um bloco lógico só pode ser mapeado para um único grupo de host de cada vez, e um determinado grupo de host não tem NSIDs duplicados.

Sobre os subsistemas NVMe

Um subsistema NVMe inclui uma ou mais controladores NVMe, namespaces, portas de subsistema NVM, um meio de storage NVM e uma interface entre a controladora e o meio de storage NVM. Quando você cria um namespace NVMe, por padrão ele não é mapeado para um subsistema. Você também pode optar por mapear um subsistema novo ou existente.

Informações relacionadas

- Aprenda a "Provisionamento de storage NVMe" usar os sistemas ASA, AFF e FAS
- Saiba mais sobre "Mapear um namespace NVMe para um subsistema"os sistemas ASA AFF e FAS.
- "Configurar hosts SAN e clientes em nuvem"

- Aprenda a "Provisionamento de storage SAN" usar os sistemas de armazenamento ASA R2 (ASA A1K, ASA A70 ou ASA A90).

Requisitos de licença NVMe

A partir do ONTAP 9.5, é necessária uma licença para dar suporte ao NVMe. Se o NVMe estiver habilitado no ONTAP 9.4, um período de carência de 90 dias será concedido para adquirir a licença após a atualização para o ONTAP 9.5.

Você pode ativar a licença usando o seguinte comando:

```
system license add -license-code NVMe_license_key
```

Configuração, suporte e limitações do NVMe

A partir do ONTAP 9.4, o "Memória expressa (NVMe) não volátil" protocolo está disponível para ambientes SAN. O FC-NVMe usa a mesma configuração física e prática de zoneamento das redes FC tradicionais, mas permite maior largura de banda, IOPs maiores e latência reduzida do que o FC-SCSI.

As limitações e o suporte do NVMe variam de acordo com a versão do ONTAP, a plataforma e a configuração. Para obter detalhes sobre sua configuração específica, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp". Para obter os limites suportados, "Hardware Universe"consulte .

> O máximo de nós por cluster está disponível no Hardware Universe em **mistura de plataformas suportadas**.

Configuração

- É possível configurar a configuração NVMe usando uma única malha ou várias malhas.
- Você deve configurar um LIF de gerenciamento para cada SVM que suporte SAN.
- O uso de malhas de switch FC heterogêneas não é suportado, exceto no caso de switches blade incorporados.

  Exceções específicas estão listadas no "Ferramenta de Matriz de interoperabilidade do NetApp".

- Cascata, malha parcial, malha completa, borda central e tecidos diretor são todos métodos padrão do setor de conexão de switches FC a uma malha e todos são compatíveis.

  Uma malha pode consistir em um ou vários switches, e os controladores de storage podem ser conectados a vários switches.

Caraterísticas

Os recursos NVMe a seguir são compatíveis com base na sua versão do ONTAP.

Começando com ONTAP…	Compatível com NVMe
9.15.1	• Configurações de IP MetroCluster de quatro nós em NVMe/TCP

9.14.1	• Definir a prioridade do host no subsistema (QoS em nível de host)
9.12.1	• Configurações de IP MetroCluster de quatro nós no NVMe/FC • As configurações do MetroCluster não são compatíveis com redes NVMe front-end anteriores ao ONTAP 9.12,1. • As configurações do MetroCluster não são compatíveis com NVMe/TCP.
9.10.1	Redimensionamento de um namespace
9.9.1	• Coexistência de namespaces e LUNs no mesmo volume
9,8	• Coexistência do protocolo Os protocolos SCSI, nas e NVMe podem existir na mesma máquina virtual de storage (SVM). Antes do ONTAP 9.8, o NVMe pode ser o único protocolo na SVM.
9,6	• blocos de 512 bytes e blocos de 4096 bytes para namespaces 4096 é o valor padrão. 512 só deve ser usado se o sistema operacional host não suportar blocos de 4096 bytes. • Movimentação de volume com namespaces mapeados
9,5	• Failover de par de HA multipath/giveback

Protocolos

Os protocolos NVMe a seguir são compatíveis.

Protocolo	Começando com ONTAP…	Permitido por…
TCP	9.10.1	Padrão
FC	9,4	Padrão

A partir do ONTAP 9.8, é possível configurar protocolos SCSI, nas e NVMe na mesma máquina virtual de storage (SVM). No ONTAP 9.7 e versões anteriores, o NVMe pode ser o único protocolo na SVM.

Namespaces

Ao trabalhar com namespaces NVMe, você deve estar ciente do seguinte:

- O ONTAP não é compatível com o comando NVMe dataset Management (desalocar) com o NVMe para exigência de espaço.
- Não é possível usar o SnapRestore para restaurar um namespace de um LUN ou vice-versa.
- A garantia de espaço para namespaces é a mesma que a garantia de espaço do volume contendo.
- Não é possível criar um namespace em uma transição de volume do Data ONTAP operando no modo 7D.
- Namespaces não suportam o seguinte:
  - Renomeação
  - Movimento entre volumes
  - Cópia entre volumes
  - Cópia sob demanda

Limitações adicionais

Os seguintes recursos do ONTAP não são compatíveis com configurações NVMe:

- Sincronização ativa do SnapMirror
- Console de armazenamento virtual
- Reservas persistentes

O seguinte aplica-se apenas aos nós que executam o ONTAP 9.4:

- Os LIFs e namespaces NVMe devem ser hospedados no mesmo nó.
- O serviço NVMe deve ser criado antes da criação do NVMe LIF.

Informações relacionadas

"Práticas recomendadas para SAN moderna"

Configurar uma VM de storage para NVMe

Para usar o protocolo NVMe em um nó, configure o SVM especificamente para NVMe.

Antes de começar

Seus adaptadores FC ou Ethernet devem ser compatíveis com NVMe. Os adaptadores suportados estão listados no "NetApp Hardware Universe".

Exemplo 3. Passos

System Manager

Configurar uma VM de storage para NVMe com o ONTAP System Manager (9,7 e posterior).

Para configurar o NVMe em uma nova VM de storage	Para configurar o NVMe em uma VM de storage existente
1. No System Manager, clique em **Storage > Storage VMs** e, em seguida, clique em **Add**. 2. Introduza um nome para a VM de armazenamento. 3. Selecione **NVMe** para o **Access Protocol**. 4. Selecione **Ativar NVMe/FC** ou **Ativar NVMe/TCP** e **Salvar**.	1. No System Manager, clique em **Storage > Storage VMs**. 2. Clique na VM de armazenamento que você deseja configurar. 3. Clique na guia **Configurações** e, em seguida, clique ⚙ ao lado do protocolo NVMe. 4. Selecione **Ativar NVMe/FC** ou **Ativar NVMe/TCP** e **Salvar**.

CLI

Configurar uma VM de storage para NVMe com a CLI do ONTAP.

1. Se você não quiser usar um SVM existente, crie um:

```
vserver create -vserver <SVM_name>
```

   a. Verifique se o SVM foi criado:

```
vserver show
```

2. Verifique se você tem adaptadores compatíveis com NVMe ou TCP instalados no cluster:

   Para NVMe:

```
network fcp adapter show -data-protocols-supported fc-nvme
```

   Para TCP:

```
network port show
```

3. Se você estiver executando o ONTAP 9.7 ou anterior, remova todos os protocolos do SVM:

```
vserver remove-protocols -vserver <SVM_name> -protocols
iscsi,fcp,nfs,cifs,ndmp
```

A partir do ONTAP 9.8, não é necessário remover outros protocolos ao adicionar o NVMe.

4. Adicionar o protocolo NVMe à SVM:

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. Se você estiver executando o ONTAP 9.7 ou anterior, verifique se o NVMe é o único protocolo permitido no SVM:

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

O NVMe deve ser o único protocolo exibido sob a `allowed protocols` coluna.

6. Criar o serviço NVMe:

```
vserver nvme create -vserver <SVM_name>
```

7. Verifique se o serviço NVMe foi criado:

```
vserver nvme show -vserver <SVM_name>
```

O `Administrative Status` do SVM deve ser listado como `up`.

8. Criar um LIF NVMe/FC:
   - Para ONTAP 9.9,1 ou anterior, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -role data -data
-protocol fc-nvme -home-node <home_node> -home-port <home_port>
```

   - Para ONTAP 9.10,1 ou posterior, FC ou TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp | default-data-nvme-fc> -data-protocol
<fcp | fc-nvme | nvme-tcp> -home-node <home_node> -home-port
<home_port> -status-admin up -failover-policy disabled -firewall
-policy data -auto-revert false -failover-group <failover_group>
-is-dns-update-enabled false
```

9. Crie um NVMe/FC LIF no nó de parceiro de HA:

- Para ONTAP 9.9,1 ou anterior, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

- Para ONTAP 9.10,1 ou posterior, FC ou TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fcp | fc-nvme | nvme-tcp> -home-node <home_node>
-home-port <home_port> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false -failover-group
<failover_group> -is-dns-update-enabled false
```

10. Verifique se os LIFs NVMe/FC foram criados:

```
network interface show -vserver <SVM_name>
```

11. Criar volume no mesmo nó que o LIF:

```
vol create -vserver <SVM_name> -volume <vol_name> -aggregate
<aggregate_name> -size <volume_size>
```

Se for apresentada uma mensagem de aviso sobre a política de eficiência automática, esta pode ser ignorada com segurança.

Provisionamento de storage NVMe

Use estas etapas para criar namespaces e provisionar storage para qualquer host compatível com NVMe em uma VM de storage existente.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para provisionar seu storage. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

A partir do ONTAP 9.8, quando você provisiona o storage, a QoS é habilitada por padrão. Você pode desativar o QoS ou escolher uma política de QoS personalizada durante o processo de provisionamento ou posteriormente.

Antes de começar

Sua VM de storage deve estar configurada para NVMe, e seu transporte FC ou TCP já deve estar configurado.

System Manager

Usando o Gerenciador de sistemas do ONTAP (9,7 e posterior), crie namespaces para fornecer storage usando o protocolo NVMe.

Passos

1. No System Manager, clique em **Storage > NVMe Namespaces** e, em seguida, clique em **Add**.

   Se precisar criar um novo subsistema, clique em **mais Opções**.

2. Se você estiver executando o ONTAP 9.8 ou posterior e quiser desativar o QoS ou escolher uma política de QoS personalizada, clique em **mais opções** e, em **armazenamento e otimização**, selecione **nível de serviço de desempenho**.
3. Coloque as suas centrais FC por WWPN. Use uma zona por iniciador e inclua todas as portas de destino em cada zona.
4. No seu host, descubra os novos namespaces.
5. Inicialize o namespace e formate-o com um sistema de arquivos.
6. Verifique se o host pode gravar e ler dados no namespace.

CLI

Com a CLI do ONTAP, crie namespaces para fornecer storage usando o protocolo NVMe.

Esse procedimento cria um namespace e um subsistema NVMe em uma VM de storage existente que já foi configurada para o protocolo NVMe e, em seguida, mapeia o namespace para o subsistema para permitir acesso a dados do sistema host.

Se precisar configurar a VM de storage para NVMe, "Configurar um SVM para NVMe"consulte .

Passos

1. Verifique se o SVM está configurado para NVMe:

   ```
   vserver show -vserver <svm_name> -fields allowed-protocols
   ```

   `NVMe` deve ser exibido sob a `allowed-protocols` coluna.

2. Crie o namespace NVMe:

   > O volume que você faz referência com o `-path` parâmetro já deve existir ou você precisará criar um antes de executar este comando.

   ```
   vserver nvme namespace create -vserver <svm_name> -path <path> -size
   <size_of_namespace> -ostype <OS_type>
   ```

3. Crie o subsistema NVMe:

```
vserver nvme subsystem create -vserver <svm_name> -subsystem
<name_of_subsystem> -ostype <OS_type>
```

O nome do subsistema NVMe diferencia maiúsculas de minúsculas. Deve conter 1 a 96 carateres. Carateres especiais são permitidos.

4. Verifique se o subsistema foi criado:

```
vserver nvme subsystem show -vserver <svm_name>
```

O `nvme` subsistema deve ser exibido sob a `Subsystem` coluna.

5. Obtenha o NQN do host.
6. Adicione o NQN do host ao subsistema:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN>
```

7. Mapeie o namespace para o subsistema:

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem
<subsystem_name> -path <path>
```

Um namespace só pode ser mapeado para um único subsistema.

8. Verifique se o namespace está mapeado para o subsistema:

```
vserver nvme namespace show -vserver <svm_name> -instance
```

O subsistema deve ser listado como `Attached subsystem` .

Mapear um namespace NVMe para um subsistema

O mapeamento de um namespace NVMe para um subsistema permite acesso aos dados do seu host. É possível mapear um namespace NVMe para um subsistema quando você provisiona o storage ou pode fazê-lo depois que o storage tiver sido provisionado.

A partir do ONTAP 9.14,1, você pode priorizar a alocação de recursos para hosts específicos. Por padrão, quando um host é adicionado ao subsistema NVMe, ele recebe prioridade regular. Você pode usar a interface de linha de comando (CLI) do ONTAP para alterar manualmente a prioridade padrão de regular para alta. Os hosts atribuídos a uma alta prioridade são alocadas contagens de filas de e/S maiores e profundidades de

filas.

Se você quiser dar uma alta prioridade a um host que foi adicionado a um subsistema no ONTAP 9.13,1 ou anterior, você pode altere a prioridade do host.

Antes de começar

Seu namespace e subsistema já devem ser criados. Se precisar criar um namespace e um subsistema, "Provisionamento de storage NVMe"consulte .

Passos

1. Obtenha o NQN do host.
2. Adicione o NQN do host ao subsistema:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
```

Se você quiser alterar a prioridade padrão do host de regular para alta, use a `-priority high` opção. Esta opção está disponível a partir de ONTAP 9.14,1.

3. Mapeie o namespace para o subsistema:

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem
<subsystem_name> -path <path>
```

Um namespace só pode ser mapeado para um único subsistema.

4. Verifique se o namespace está mapeado para o subsistema:

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

O subsistema deve ser listado como `Attached subsystem` .

Gerenciar LUNs

Editar grupo de políticas de QoS LUN

A partir do ONTAP 9.10,1, você pode usar o Gerenciador de sistema para atribuir ou remover políticas de qualidade do serviço (QoS) em vários LUNs ao mesmo tempo.

Se a política de QoS for atribuída ao nível do volume, ela deverá ser alterada no nível do volume. Você só pode editar a política de QoS no nível LUN se ela foi originalmente atribuída no nível LUN.

Passos

1. No System Manager, clique em **Storage > LUNs**.

2. Selecione o LUN ou LUNs que pretende editar.

   Se você estiver editando mais de um LUN de cada vez, os LUNs devem pertencer à mesma Máquina Virtual de Storage (SVM). Se você selecionar LUNs que não pertençam ao mesmo SVM, a opção de editar o Grupo de políticas de QoS não será exibida.

3. Clique em **mais** e selecione **Editar Grupo de políticas de QoS**.

Converta um LUN em um namespace

A partir do ONTAP 9.11,1, você pode usar a CLI do ONTAP para converter no local um LUN existente em um namespace NVMe.

Antes de começar

- LUN especificado não deve ter nenhum mapa existente para um grupo.
- O LUN não deve estar em um SVM configurado pelo MetroCluster ou em uma relação de sincronização ativa do SnapMirror.
- O LUN não deve ser um endpoint de protocolo ou vinculado a um endpoint de protocolo.
- O LUN não deve ter um prefixo e/ou fluxo de sufixo não zero.
- O LUN não deve fazer parte de um instantâneo ou no lado de destino da relação do SnapMirror como um LUN somente leitura.

Passo

1. Converter um LUN para um namespace NVMe:

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```

Tire um LUN off-line

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para colocar LUNs off-line. Antes do ONTAP 9.10,1, você deve usar a CLI do ONTAP para colocar LUNs off-line.

System Manager

Passos

1. No System Manager, clique em **Storage>LUNs**.
2. Coloque um único LUN ou vários LUNs offline

Se você quiser…	Faça isso…
Tire um único LUN off-line	Ao lado do nome do LUN, clique ⋮ e selecione **Take Offline**.
Coloque vários LUNs offline	1. Selecione os LUNs que pretende colocar offline. 2. Clique em **More** e selecione **Take Offline**.

CLI

Você só pode colocar um LUN off-line de cada vez ao usar a CLI.

Passo

1. Coloque o LUN offline:

```
lun offline <lun_name> -vserver <SVM_name>
```

Redimensione um LUN no ONTAP

Pode aumentar ou diminuir o tamanho de um LUN.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para aumentar o tamanho de uma unidade de armazenamento. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

ⓘ Os LUNs Solaris não podem ser redimensionados.

Aumente o tamanho de um LUN

O tamanho para o qual você pode aumentar seu LUN varia dependendo da sua versão do ONTAP.

Versão de ONTAP	Tamanho máximo de LUN
ONTAP 9.12.1P2 e posterior	128 TB para plataformas AFF, FAS e ASA

ONTAP 9 F.8 e mais tarde	• 128 TB para plataformas All-Flash SAN Array (ASA) • 16 TB para plataformas não ASA
ONTAP 9.5, 9,6, 9,7	16 TB
ONTAP 9 .4 ou anterior	10 vezes o tamanho original do LUN, mas não superior a 16TB, que é o tamanho máximo do LUN. Por exemplo, se você criar um LUN de 100 GB, só poderá aumentá-lo para 1.000 GB. O tamanho máximo real do LUN pode não ser exatamente 16TB. ONTAP arredonda o limite para ser um pouco menos.

Você não precisa colocar o LUN off-line para aumentar o tamanho. No entanto, depois de aumentar o tamanho, você deve redigitalizar o LUN no host para que o host reconheça a alteração de tamanho.

Saiba mais sobre `lun resize` o "Referência do comando ONTAP"na .

Exemplo 4. Passos

System Manager

Aumente o tamanho de um LUN com o ONTAP System Manager (9,7 e posterior).

1. No System Manager, clique em **Storage > LUNs**.
2. Clique ⋮ e selecione **Editar**.
3. Em **armazenamento e Otimização** aumente o tamanho do LUN e **Salvar**.

CLI

Aumente o tamanho de um LUN com a CLI do ONTAP.

1. Aumente o tamanho do LUN:

```
lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
-size <lun_size>
```

2. Verifique o tamanho de LUN aumentado:

```
lun show -vserver <SVM_name>
```

As operações de ONTAP resumem o tamanho máximo real do LUN para que ele seja ligeiramente menor do que o valor esperado. Além disso, o tamanho real do LUN pode variar ligeiramente com base no tipo de SO do LUN. Para obter o valor exato redimensionado, execute os seguintes comandos no modo avançado:

```
set -unit B

lun show -fields max-resize-size -volume volume_name -lun lun_name
```

1. Volte a digitalizar o LUN no host.
2. Siga a documentação do host para tornar o tamanho LUN recém-criado visível para o sistema de arquivos do host.

Diminua o tamanho de um LUN

Antes de diminuir o tamanho de um LUN, o host precisa migrar os blocos que contêm os dados de LUN para o limite do tamanho de LUN menor. Você deve usar uma ferramenta como o SnapCenter para garantir que o LUN seja diminuído corretamente sem truncar blocos contendo dados de LUN. Diminuir manualmente o tamanho do LUN não é recomendado.

Depois de diminuir o tamanho do LUN, o ONTAP notifica automaticamente o iniciador de que o tamanho do LUN diminuiu. No entanto, podem ser necessárias etapas adicionais no seu host para que o host reconheça o novo tamanho de LUN. Verifique a documentação do host para obter informações específicas sobre como diminuir o tamanho da estrutura do arquivo host.

Mover um LUN

Você pode mover um LUN entre volumes em uma máquina virtual de storage (SVM), mas não pode mover um LUN entre SVMs. As LUNs migradas em volumes dentro de uma SVM são movidas imediatamente e sem perda de conectividade.

O que você vai precisar

Se o LUN estiver usando o mapa de LUN seletivo (SLM), você deve "Modifique a lista de nós de relatórios SLM"incluir o nó de destino e seu parceiro de HA antes de mover o LUN.

Sobre esta tarefa

Os recursos de eficiência de storage, como deduplicação, compressão e compactação, não são preservados durante a movimentação de LUN. Eles devem ser reaplicados depois que a movimentação de LUN for concluída.

A proteção de dados com cópias Snapshot ocorre no nível do volume. Portanto, quando você move um LUN, ele se enquadra no esquema de proteção de dados do volume de destino. Se você não tiver cópias Snapshot estabelecidas para o volume de destino, as cópias Snapshot do LUN não serão criadas. Além disso, todas as cópias Snapshot do LUN permanecem no volume original até que essas cópias snapshot sejam excluídas.

Não é possível mover um LUN para os seguintes volumes:

- Um volume de destino SnapMirror
- Volume raiz do SVM

Não é possível mover os seguintes tipos de LUNs:

- Um LUN que foi criado a partir de um ficheiro
- Um LUN que está no estado NVFail
- Um LUN que está em um relacionamento de compartilhamento de carga
- Um LUN de classe de endpoint de protocolo

Para LUNs Solaris os_type que tenham 1 TB ou mais, o host pode ter um tempo limite durante a movimentação de LUN. Para esse tipo de LUN, você deve desmontar o LUN antes de iniciar a movimentação.

Exemplo 5. Passos

System Manager

Mova um LUN com o Gerenciador de sistema do ONTAP (9,7 e posterior).

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para criar um novo volume ao mover um único LUN. No ONTAP 9 1 e 9,9.8, o volume para o qual você está movendo seu LUN deve existir antes de iniciar a movimentação do LUN.

Passos

1. No System Manager, clique em **Storage>LUNs**.
2. Clique com o botão direito do rato no LUN que pretende mover e, em seguida, clique ⋮ em **mover LUN**.

   No ONTAP 9.10,1, selecione para mover o LUN para **um volume existente** ou para um **novo volume**.

   Se você selecionar para criar um novo volume, forneça as especificações de volume.
3. Clique em **mover**.

CLI

Mova um LUN com a CLI do ONTAP.

1. Mover o LUN:

   ```
   lun move start
   ```

   Durante um período muito breve, o LUN é visível tanto no volume de origem como no de destino. Isso é esperado e é resolvido após a conclusão da mudança.
2. Acompanhe o status da movimentação e verifique a conclusão bem-sucedida:

   ```
   lun move show
   ```

Informações relacionadas

- "Mapa LUN seletivo"

Eliminar LUNs

Você pode excluir um LUN de uma máquina virtual de storage (SVM) se não precisar mais do LUN.

O que você vai precisar

O LUN deve ser desmapeado do seu grupo antes de poder excluí-lo.

Passos

1. Verifique se o aplicativo ou o host não está usando o LUN.
2. Desmapeie o LUN do grupo:

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<LUN_name> -igroup <igroup_name>
```

3. Eliminar o LUN:

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. Verifique se você excluiu o LUN:

```
lun show -vserver <SVM_name>
```

```
Vserver   Path              State    Mapped  Type     Size
--------- ----------------- -------- ------- -------- ------
vs5       /vol/vol16/lun8   online   mapped  windows  10.00GB
```

O que saber antes de copiar LUNs

Você deve estar ciente de certas coisas antes de copiar um LUN.

Os administradores de cluster podem copiar um LUN entre máquinas virtuais de armazenamento (SVMs) dentro do cluster usando o `lun copy` comando. Os administradores de cluster devem estabelecer a relação de peering de máquina virtual de storage (SVM) usando o comando antes de uma operação de cópia LUN entre SVM `vserver peer create` ser executada. Deve haver espaço suficiente no volume de origem para um clone SIS.

LUNs nas cópias Snapshot podem ser usadas como LUNs de origem para o `lun copy` comando. Quando você copia um LUN usando o `lun copy` comando, a cópia LUN fica imediatamente disponível para acesso de leitura e gravação. O LUN de origem não é alterado pela criação de uma cópia LUN. Tanto o LUN de origem como a cópia LUN existem como LUNs exclusivos com números de série LUN diferentes. As alterações feitas no LUN de origem não são refletidas na cópia LUN e as alterações feitas na cópia LUN não são refletidas no LUN de origem. O mapeamento LUN do LUN de origem não é copiado para o novo LUN; a cópia LUN deve ser mapeada.

A proteção de dados com cópias Snapshot ocorre no nível do volume. Portanto, se você copiar um LUN para um volume diferente do volume do LUN de origem, o LUN de destino estará sob o esquema de proteção de dados do volume de destino. Se você não tiver cópias Snapshot estabelecidas para o volume de destino, as cópias Snapshot não serão criadas da cópia LUN.

Copiar LUNs é uma operação sem interrupções.

Não é possível copiar os seguintes tipos de LUNs:

- Um LUN que foi criado a partir de um ficheiro
- Um LUN que está no estado NVFAIL
- Um LUN que está em um relacionamento de compartilhamento de carga
- Um LUN de classe de endpoint de protocolo

Examine o espaço configurado e usado de um LUN

Conhecer o espaço configurado e o espaço real usado para os LUNs pode ajudá-lo a determinar a quantidade de espaço que pode ser recuperado ao fazer a recuperação de espaço, a quantidade de espaço reservado que contém dados e o tamanho total configurado em relação ao tamanho real usado para um LUN.

Passo

1. Exibir o espaço configurado versus o espaço real usado para um LUN:

   ```
   lun show
   ```

   O exemplo a seguir mostra o espaço configurado versus o espaço real usado pelas LUNs na máquina virtual de storage (SVM) VS3:

   ```
   lun show -vserver vs3 -fields path, size, size-used, space-reserve
   ```

   ```
   vserver path                    size    space-reserve size-used
   ------- ------------------      ------- ------------- ---------
   vs3     /vol/vol0/lun1          50.01GB disabled      25.00GB
   vs3     /vol/vol0/lun1_backup   50.01GB disabled      32.15GB
   vs3     /vol/vol0/lun2          75.00GB disabled      0B
   vs3     /vol/volspace/lun0      5.00GB  enabled       4.50GB
   4 entries were displayed.
   ```

Controle e monitore o desempenho de e/S para LUNs com o uso do QoS de storage

Você pode controlar a performance de entrada/saída (e/S) a LUNs atribuindo LUNs a grupos de políticas QoS de storage. Você pode controlar a performance de e/S para garantir que os workloads atinjam objetivos de performance específicos ou para controlar um workload que afeta negativamente outros workloads.

Sobre esta tarefa

Os grupos de políticas aplicam um limite máximo de taxa de transferência (por exemplo, 100 MB/s). Você pode criar um grupo de políticas sem especificar uma taxa de transferência máxima, que permite monitorar o desempenho antes de controlar a carga de trabalho.

Também é possível atribuir máquinas virtuais de storage (SVMs) a volumes e LUNs do FlexVol a grupos de políticas.

Observe os seguintes requisitos sobre a atribuição de um LUN a um grupo de políticas:

- O LUN deve estar contido pelo SVM ao qual o grupo de políticas pertence.

  Você especifica o SVM ao criar o grupo de políticas.

- Se você atribuir um LUN a um grupo de políticas, não será possível atribuir o volume ou SVM contendo LUN a um grupo de políticas.

Para obter mais informações sobre como usar QoS de armazenamento, consulte "Referência de administração do sistema".

Passos

1. Use o `qos policy-group create` comando para criar um grupo de políticas.
2. Use o `lun create` comando ou o `lun modify` comando com o `-qos-policy-group` parâmetro para atribuir um LUN a um grupo de políticas.
3. Use os `qos statistics` comandos para exibir dados de desempenho.
4. Se necessário, use o `qos policy-group modify` comando para ajustar o limite máximo de taxa de transferência do grupo de políticas.

Ferramentas disponíveis para monitorar seus LUNs de forma eficaz

Estão disponíveis ferramentas para o ajudar a monitorizar eficazmente os seus LUNs e evitar ficar sem espaço.

- O Active IQ Unified Manager é uma ferramenta gratuita que permite gerenciar todo o storage em todos os clusters do ambiente.
- O System Manager é uma interface gráfica de usuário incorporada ao ONTAP que permite gerenciar manualmente as necessidades de storage no nível do cluster.
- O OnCommand Insight apresenta uma visão única da sua infraestrutura de storage e permite configurar monitoramento automático, alertas e geração de relatórios quando LUNs, volumes e agregados estão ficando sem espaço de storage.

Funcionalidades e restrições de LUNs transicionados

Em um ambiente SAN, é necessária uma interrupção no serviço durante a transição de um volume de 7 modos para o ONTAP. Você precisa encerrar seus hosts para concluir a transição. Após a transição, você precisa atualizar as configurações de seu host antes de começar a fornecer dados no ONTAP

Você precisa agendar uma janela de manutenção durante a qual você pode encerrar seus hosts e concluir a transição.

Os LUNs transferidos do Data ONTAP que operam no modo 7 para o ONTAP têm certos recursos e restrições que afetam a maneira como os LUNs podem ser gerenciados.

Você pode fazer o seguinte com LUNs transicionados:

- Visualize o LUN usando o `lun show` comando
- Visualize o inventário de LUNs transferidos do volume do modo 7D usando o `transition 7-mode`

`show` comando

- Restaure um volume a partir de uma cópia Snapshot de 7 modos

  A restauração do volume faz a transição de todos os LUNs capturados na cópia Snapshot

- Restaure um único LUN a partir de uma cópia Snapshot de 7 modos usando o `snapshot restore-file` comando
- Crie um clone de um LUN em uma cópia Snapshot de 7 modos
- Restaure um intervalo de blocos a partir de um LUN capturado em uma cópia Snapshot de 7 modos
- Crie um FlexClone do volume usando uma cópia Snapshot do modo 7

Não é possível fazer o seguinte com LUNs transicionados:

- Acesse clones LUN com cópia Snapshot capturados no volume

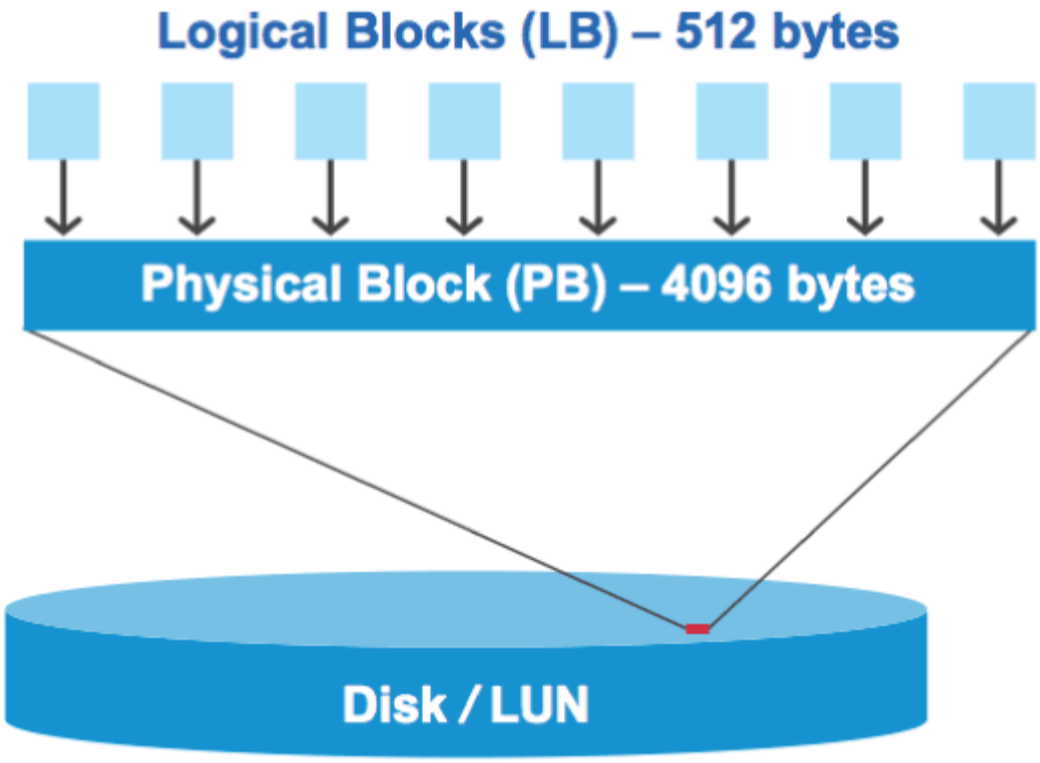
Informações relacionadas

"Transição baseada em cópia"

Desalinhamentos de e/S na visão geral dos LUNs alinhados adequadamente

O ONTAP pode relatar desalinhamentos de e/S em LUNs alinhados corretamente. Em geral, esses avisos de desalinhamento podem ser desconsiderados, desde que você esteja confiante de que seu LUN está corretamente provisionado e que sua tabela de particionamento está correta.

LUNs e discos rígidos fornecem armazenamento como blocos. Como o tamanho do bloco para discos no host é de 512 bytes, os LUNs apresentam blocos desse tamanho ao host, enquanto usam blocos maiores de 4 KB para armazenar dados. O bloco de dados de 512 bytes usado pelo host é referido como um bloco lógico. O bloco de dados de 4 KB usado pelo LUN para armazenar dados é referido como um bloco físico. Isso significa que existem oito blocos lógicos de 512 bytes em cada bloco físico de 4 KB.



O sistema operacional do host pode iniciar uma operação de e/S de leitura ou gravação em qualquer bloco lógico. As operações de e/S só são consideradas alinhadas quando começam no primeiro bloco lógico no bloco físico. Se uma operação de e/S começar em um bloco lógico que também não é o início de um bloco físico, a e/S é considerada desalinhada. O ONTAP deteta automaticamente o desalinhamento e informa-o no LUN. No entanto, a presença de e/S desalinhadas não significa necessariamente que o LUN também esteja desalinhado. É possível que e/S desalinhadas sejam relatadas em LUNs alinhados corretamente.

Se necessitar de mais investigação, consulte o artigo da base de dados de Conhecimento "Como identificar e/S desalinhadas em LUNs?"

Para obter mais informações sobre ferramentas para corrigir problemas de alinhamento, consulte a seguinte documentação

- "Utilitários do Windows Unified Host 7,1"
- "Provisione a documentação de storage SAN"

Obtenha alinhamento de e/S usando os tipos de SO LUN

Para o ONTAP 9.7 ou anterior, você deve usar o valor de LUN ONTAP `ostype` recomendado que mais corresponde ao seu sistema operacional para alcançar o alinhamento de e/S com o esquema de particionamento do sistema operacional.

O esquema de partição empregado pelo sistema operacional host é um fator importante que contribui para desalinhamentos de e/S. Alguns valores de LUN do ONTAP `ostype` usam um deslocamento especial conhecido como "prefixo" para permitir que o esquema de particionamento padrão usado pelo sistema operacional do host seja alinhado.

Em algumas circunstâncias, uma tabela de particionamento personalizada pode ser necessária para alcançar o alinhamento de e/S. No entanto, para `ostype` valores com um valor "'prefixo'" maior que `0`, uma partição personalizada pode criar e/S desalinhadas

Para obter mais informações sobre LUNs provisionados no ONTAP 9.7 ou anterior, consulte o artigo da KB "Como identificar e/S desalinhadas em LUNs".

Por padrão, os novos LUNs provisionados no ONTAP 9.8 ou posterior têm um tamanho de prefixo e sufixo de zero para todos os tipos de sistema operacional LUN. A e/S deve estar alinhada com o sistema operacional de host suportado por padrão.

Considerações especiais de alinhamento de e/S para Linux

As distribuições Linux oferecem uma ampla variedade de maneiras de usar um LUN, incluindo como dispositivos brutos para bancos de dados, vários gerenciadores de volume e sistemas de arquivos. Não é necessário criar partições em um LUN quando usado como um dispositivo bruto ou como volume físico em um volume lógico.

Para RHEL 5 e anteriores e SLES 10 e anteriores, se o LUN será usado sem um gerenciador de volume, você deve particionar o LUN para ter uma partição que começa em um deslocamento alinhado, que é um setor que é um mesmo múltiplo de oito blocos lógicos.

Considerações especiais de alinhamento de e/S para LUNs Solaris

Você precisa considerar vários fatores ao determinar se você deve usar o `solaris` ostype ou o ostype. `solaris_efi`

Consulte "Guia de instalação e administração dos Utilitários do Solaris Host" para obter informações detalhadas.

Os LUNs de inicialização do ESX relatam como desalinhados

Os LUNs usados como LUNs de inicialização do ESX geralmente são relatados pelo ONTAP como desalinhados. O ESX cria várias partições no LUN de inicialização, dificultando o alinhamento. LUNs de inicialização do ESX desalinhados geralmente não são um problema de desempenho porque a quantidade total de e/S desalinhados é pequena. Supondo que o LUN foi corretamente provisionado com o VMware `ostype`, nenhuma ação é necessária.

Informações relacionadas

"Alinhamento de partição/disco do sistema de arquivos VM convidada para VMware vSphere, outros ambientes virtuais e sistemas de storage NetApp"

Formas de resolver problemas quando os LUNs ficam offline

Quando não há espaço disponível para gravações, os LUNs ficam offline para preservar a integridade dos dados. Os LUNs podem ficar sem espaço e ficar offline por vários motivos, e há várias maneiras de resolver o problema.

Se o…	Você pode…
O agregado está cheio	• Adicione mais discos. • Use o `volume modify` comando para reduzir um volume que tenha espaço disponível. • Se você tiver volumes de garantia de espaço que tenham espaço disponível, altere a garantia de espaço de volume para `none` com o `volume modify` comando.
O volume está cheio, mas há espaço disponível no agregado contendo	• Para volumes de garantia de espaço, use o `volume modify` comando para aumentar o tamanho do seu volume. • Para volumes provisionados de forma fina, use o `volume modify` comando para aumentar o tamanho máximo do seu volume. Se o volume com crescimento automático não estiver ativado, `volume modify -autogrow -mode` utilize para o ativar. • Exclua cópias Snapshot manualmente com o `volume snapshot delete` comando ou use o `volume snapshot autodelete modify` comando para excluir cópias snapshot automaticamente.

Informações relacionadas

"Gerenciamento de disco e camada local (agregado)"

"Gerenciamento de storage lógico"

Solucionar problemas de LUNs iSCSI não visíveis no host

Os iSCSI LUNs aparecem como discos locais para o host. Se os LUNs do sistema de armazenamento não estiverem disponíveis como discos no host, você deverá verificar as configurações.

Definição de configuração	O que fazer
Cabeamento	Verifique se os cabos entre o host e o sistema de armazenamento estão conetados corretamente.

Definição de configuração	O que fazer
Conetividade de rede	Verifique se há conetividade TCP/IP entre o host e o sistema de armazenamento. • Na linha de comando do sistema de storage, faça ping nas interfaces de host que estão sendo usadas para iSCSI: `ping -node` *`node_name`* `-destination` *`host_ip_address_for_iSCSI`* • Na linha de comando do host, faça ping nas interfaces do sistema de storage que estão sendo usadas para iSCSI: `ping -node` *`node_name`* `-destination` *`host_ip_address_for_iSCSI`*
Requisitos do sistema	Verifique se os componentes da sua configuração estão qualificados. Além disso, verifique se você tem o nível correto de Service pack do sistema operacional do host (SO), a versão do iniciador, a versão do ONTAP e outros requisitos do sistema. A Matriz de interoperabilidade contém os requisitos de sistema mais atualizados.
Jumbo Frames	Se você estiver usando quadros jumbo em sua configuração, verifique se os quadros jumbo estão ativados em todos os dispositivos no caminho de rede: A NIC Ethernet do host, o sistema de armazenamento e quaisquer switches.
Estado do serviço iSCSI	Verifique se o serviço iSCSI está licenciado e iniciado no sistema de armazenamento.
Início de sessão do iniciador	Verifique se o iniciador está conetado ao sistema de armazenamento. Se o `iscsi initiator show` comando output não mostrar que nenhum iniciador está conetado, verifique a configuração do iniciador no host. Verifique também se o sistema de armazenamento está configurado como um destino do iniciador.
Nomes de nós iSCSI (IQNs)	Verifique se você está usando os nomes de nó do iniciador corretos na configuração do igroup. No host, você pode usar as ferramentas e os comandos do iniciador para exibir o nome do nó do iniciador. Os nomes de nós do iniciador configurados no grupo e no host devem corresponder.
Mapeamentos LUN	Verifique se os LUNs estão mapeados para um grupo. No console do sistema de storage, você pode usar um dos seguintes comandos: • `lun mapping show` Exibe todos os LUNs e os grupos para os quais são mapeados. • `lun mapping show -igroup` Exibe os LUNs mapeados para um grupo específico.
ISCSI LIFs habilitadas	Verifique se as interfaces lógicas iSCSI estão ativadas.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

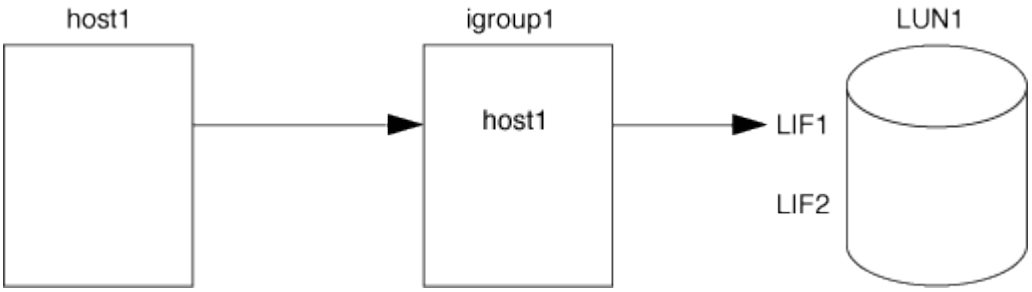
Gerencie grupos e portsets

Maneiras de limitar o acesso LUN com portsets e grupos

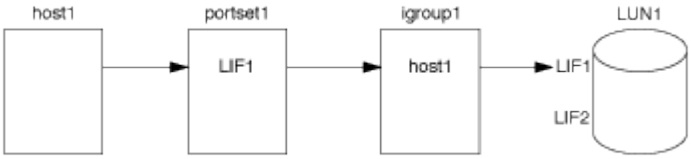
Além de usar o mapa LUN Seletivo (SLM), você pode limitar o acesso aos LUNs por meio de grupos e portsets.

Os Portsets podem ser usados com o SLM para restringir ainda mais o acesso de determinados alvos a certos iniciadores. Ao usar o SLM com portsets, os LUNs estarão acessíveis no conjunto de LIFs no portset no nó proprietário do LUN e no parceiro de HA desse nó.

No exemplo a seguir, initiator1 não tem um portset Sem um portset, initiator1 pode acessar LUN1 através de LIF1 e LIF2.



Você pode limitar o acesso ao LUN1 usando um portset No exemplo a seguir, o initiator1 pode acessar o LUN1 somente através do LIF1. No entanto, o initiator1 não pode acessar o LUN1 através do LIF2 porque o LIF2 não está no portset1.



Informações relacionadas

- Mapa LUN seletivo
- Criar um portset e ligar a um igroup

Visualizar e gerenciar iniciadores e grupos SAN

Você pode usar o System Manager para exibir e gerenciar grupos de iniciadores (grupos de iniciadores) e iniciadores.

Sobre esta tarefa

- Os grupos de iniciadores identificam quais hosts são capazes de acessar LUNs específicos no sistema de storage.
- Depois que um grupo de iniciadores e iniciadores forem criados, você também pode editá-los ou excluí-los.
- Para gerenciar grupos e iniciadores de SAN, você pode executar as seguintes tarefas:

- [view-manage-san-igroups]
- [view-manage-san-inits]

Exibir e gerenciar grupos de iniciadores SAN

Você pode usar o System Manager para exibir uma lista de grupos de iniciadores (grupos de iniciadores). Na lista, você pode executar operações adicionais.

Passos

1. No System Manager, clique em **hosts > SAN Initiator Groups**.

   A página exibe uma lista de grupos de iniciadores (grupos de iniciadores). Se a lista for grande, você pode visualizar páginas adicionais da lista clicando nos números de página no canto inferior direito da página.

   As colunas exibem várias informações sobre os grupos. A partir de 9.11.1, o estado da ligação do grupo também é apresentado. Passe o Mouse sobre alertas de status para ver detalhes.

2. (Opcional): Você pode executar as seguintes tarefas clicando nos ícones no canto superior direito da lista:
   - **Pesquisa**
   - * Faça o download* da lista.
   - **Mostrar** ou **Ocultar** colunas na lista.
   - **Filtrar** os dados da lista.
3. Pode efetuar operações a partir da lista:
   - Clique + Add para adicionar um grupo.
   - Clique no nome do grupo para visualizar a página **Visão geral** que mostra detalhes sobre o grupo.

     Na página **Visão geral**, você pode exibir os LUNs associados ao grupo e iniciar as operações para criar LUNs e mapear os LUNs. Clique em **todos os iniciadores de SAN** para retornar à lista principal.
   - Passe o Mouse sobre o grupo e clique ⋮ ao lado de um nome do grupo para editar ou excluir o grupo.
   - Passe o Mouse sobre a área à esquerda do nome do grupo e marque a caixa de seleção. Se você clicar em * Adicionar ao Grupo Iniciador*, você pode adicionar esse grupo a outro grupo.
   - Na coluna **Storage VM**, clique no nome de uma VM de armazenamento para exibir detalhes sobre ela.

Exibir e gerenciar iniciadores de SAN

Você pode usar o System Manager para exibir uma lista de iniciadores. Na lista, você pode executar operações adicionais.

Passos

1. No System Manager, clique em **hosts > SAN Initiator Groups**.

   A página exibe uma lista de grupos de iniciadores (grupos de iniciadores).

2. Para visualizar os iniciadores, execute o seguinte:
   - Clique na guia **iniciadores FC** para exibir uma lista de iniciadores FC.
   - Clique no separador **iniciadores iSCSI** para ver uma lista de iniciadores iSCSI.

As colunas exibem várias informações sobre os iniciadores.

A partir de 9.11.1, o estado da ligação do iniciador também é apresentado. Passe o Mouse sobre alertas de status para ver detalhes.

3. (Opcional): Você pode executar as seguintes tarefas clicando nos ícones no canto superior direito da lista:
   - **Pesquisar** a lista de iniciadores específicos.
   - * Faça o download* da lista.
   - **Mostrar** ou **Ocultar** colunas na lista.
   - **Filtrar** os dados da lista.

Crie um grupo aninhado

A partir do ONTAP 9.9,1, você pode criar um grupo que consiste em outros grupos existentes.

1. No System Manager, clique em **Host > SAN Initiator Groups** e, em seguida, clique em **Add**.
2. Digite o grupo **Nome** e **Descrição**.

   A descrição serve como o alias do igroup.

3. Selecione **Storage VM** e **Host Operating System**.

   O tipo de SO de um grupo aninhado não pode ser alterado depois que o grupo é criado.

4. Em **Membros do Grupo Iniciador** selecione **Grupo de iniciadores existente**.

   Você pode usar **Search** para localizar e selecionar os grupos de iniciadores que deseja adicionar.

Mapeie grupos para vários LUNs

A partir do ONTAP 9.9,1, é possível mapear grupos para dois ou mais LUNs simultaneamente.

1. No System Manager, clique em **Storage > LUNs**.
2. Selecione os LUNs que pretende mapear.
3. Clique em **mais** e, em seguida, clique em **Map to Initiator Groups**.

Os grupos selecionados são adicionados aos LUNs selecionados. Os mapeamentos pré-existentes não são sobrescritos.

Criar um portset e ligar a um igroup

Além de usar "Mapa LUN seletivo (SLM)"o , você pode criar um portset e vincular o portset a um grupo para limitar ainda mais os LIFs que podem ser usados por um iniciador para acessar um LUN.

Se você não vincular um portset a um grupo, todos os iniciadores do grupo podem acessar LUNs mapeados através de todas as LIFs no nó que possui o LUN e o parceiro HA do nó proprietário.

O que você vai precisar

Você deve ter pelo menos um LIF e um igrop.

A menos que você esteja usando grupos de interface, dois LIFs são recomendados para redundância para iSCSI e FC. Apenas um LIF é recomendado para grupos de interfaces.

Sobre esta tarefa

É vantajoso usar portsets com SLM quando você tem mais de duas LIFs em um nó e você deseja restringir um determinado iniciador a um subconjunto de LIFs. Sem portsets, todos os destinos no nó serão acessíveis por todos os iniciadores com acesso ao LUN por meio do nó proprietário do LUN e do parceiro de HA do nó proprietário.

Exemplo 6. Passos

System Manager

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para criar portsets e vinculá-los aos grupos.

Se você precisar criar um portset e vinculá-lo a um grupo em uma versão do ONTAP anterior a 9.10.1, você deve usar o procedimento da CLI do ONTAP.

1. No System Manager, clique em **Network > Overview > Portsets** e clique em **Add**.
2. Insira as informações para o novo portset e clique em **Add**.
3. Clique em **hosts > SAN Initiator Groups**.
4. Para ligar o portset a um novo grupo, clique em **Add**.

   Para vincular o portset a um grupo existente, selecione o grupo, clique em e, em seguida, clique em **Edit Initiator Group** (Editar grupo de iniciadores).

Informações relacionadas

"Visualizar e gerenciar iniciadores e grupos de trabalho"

CLI

1. Crie um conjunto de portas contendo os LIFs apropriados:

   `portset create -vserver` *`vserver_name`* `-portset` *`portset_name`* `-protocol` *`protocol`* `-port-name` *`port_name`*

   Se estiver usando FC, especifique o `protocol` parâmetro como `fcp`. Se estiver a utilizar iSCSI, especifique o `protocol` parâmetro como `iscsi`.

2. Vincule o grupo ao conjunto de portas:

   `lun igroup bind -vserver` *`vserver_name`* `-igroup` *`igroup_name`* `-portset` *`portset_name`*

3. Verifique se os conjuntos de portas e LIFs estão corretos:

   `portset show -vserver` *`vserver_name`*

```
Vserver   Portset   Protocol Port Names    Igroups
--------- --------- -------- ------------- --------
vs3       portset0  iscsi    lif0,lif1     igroup1
```

Gerenciar portsets

Além "Mapa LUN seletivo (SLM)"do , você pode usar portsets para limitar ainda mais quais LIFs podem ser usados por um iniciador para acessar um LUN.

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para alterar as interfaces de rede

associadas a portsets e excluir portsets.

Altere as interfaces de rede associadas a um portset

1. No System Manager, selecione **rede > Visão geral > Portsets**.
2. Selecione o portset que pretende editar e, em seguida, selecione **Editar conjunto de portas**.

Eliminar um portset

1. No System Manager, clique em **rede > Visão geral > Portsets**.
2. Para eliminar um único portset, selecione o portset, selecione e, em seguida, selecione **Delete Portsets**.

   Para excluir vários portsets, selecione os portsets e clique em **Excluir**.

Descrição geral do mapa LUN seletivo

O mapa de LUN seletivo (SLM) reduz o número de caminhos do host para o LUN. Com o SLM, quando um novo mapa LUN é criado, o LUN só pode ser acessado por meio de caminhos no nó proprietário do LUN e de seu parceiro de HA.

O SLM permite o gerenciamento de um único grupo por host e também é compatível com operações de movimentação de LUN ininterruptas que não exigem manipulação de portset ou remapeamento de LUN.

"Portsets" Pode ser usado com o SLM para restringir ainda mais o acesso de determinados alvos a certos iniciadores. Ao usar o SLM com portsets, os LUNs estarão acessíveis no conjunto de LIFs no portset no nó proprietário do LUN e no parceiro de HA desse nó.

O SLM está ativado por predefinição em todos os novos mapas LUN.

Determine se o SLM está habilitado em um mapa LUN

Se o seu ambiente tiver uma combinação de LUNs criadas em uma versão do ONTAP 9 e LUNs transferidos de versões anteriores, talvez seja necessário determinar se o mapa de LUN seletivo (SLM) está habilitado em um LUN específico.

Você pode usar as informações exibidas na saída do `lun mapping show -fields reporting-nodes, node` comando para determinar se o SLM está habilitado no mapa LUN. Se o SLM não estiver habilitado, "-" será exibido nas células sob a coluna "'reportar nós'" da saída do comando. Se o SLM estiver ativado, a lista de nós exibida sob a coluna "'nós'" será duplicada na coluna "'reportar nós'".

Modifique a lista de nós de relatórios SLM

Se você estiver movendo um LUN ou um volume contendo LUNs para outro par de alta disponibilidade (HA) dentro do mesmo cluster, você deve modificar a lista de nós de relatórios de mapa de LUN seletivo (SLM) antes de iniciar a movimentação para garantir que os caminhos de LUN ativos e otimizados sejam mantidos.

Passos

1. Adicione o nó de destino e o nó de parceiro à lista de nós de relatório do agregado ou do volume:

```
lun mapping add-reporting-nodes -vserver <vserver_name> -path <lun_path>
-igroup <igroup_name> [-destination-aggregate <aggregate_name>|-
destination-volume <volume_name>]
```

Se você tiver uma convenção de nomenclatura consistente, poderá modificar vários mapeamentos de LUN ao mesmo tempo usando `igroup_prefix*` em vez `igroup_name` de .

2. Volte a digitalizar o host para descobrir os caminhos recém-adicionados.
3. Se o seu sistema operacional exigir isso, adicione os novos caminhos à configuração de e/S de rede multipath (MPIO).
4. Execute o comando para a operação de movimentação necessária e aguarde até que a operação termine.
5. Verifique se a e/S está sendo atendida pelo caminho Ativo/otimizado:

```
lun mapping show -fields reporting-nodes
```

6. Remova o proprietário do LUN anterior e o nó de parceiro da lista de nós de relatórios:

```
lun mapping remove-reporting-nodes -vserver <vserver_name> -path
<lun_path> -igroup <igroup_name> -remote-nodes
```

7. Verifique se o LUN foi removido do mapa LUN existente:

```
lun mapping show -fields reporting-nodes
```

8. Remova quaisquer entradas de dispositivo obsoletas para o sistema operacional do host.
9. Altere quaisquer arquivos de configuração de multipathing, se necessário.
10. Volte a digitalizar o host para verificar a remoção de caminhos antigos. Consulte a documentação do seu host para obter etapas específicas para verificar novamente seus hosts.

Gerir protocolo iSCSI

Configure a rede para obter o melhor desempenho

As redes Ethernet variam muito no desempenho. Pode maximizar o desempenho da rede utilizada para iSCSI selecionando valores de configuração específicos.

Passos

1. Conete o host e as portas de armazenamento à mesma rede.

   É melhor conetar-se aos mesmos interrutores. O roteamento nunca deve ser usado.

2. Selecione as portas de velocidade mais alta disponíveis e dedique-as ao iSCSI.

   As portas de 10 GbE são as melhores. As portas de 1 GbE são o mínimo.

3. Desative o controle de fluxo Ethernet para todas as portas.

   Você deve ver "Gerenciamento de rede" para usar a CLI para configurar o controle de fluxo da porta Ethernet.

4. Ative quadros jumbo (normalmente MTU de 9000).

   Todos os dispositivos no caminho de dados, incluindo iniciadores, destinos e switches, devem suportar quadros jumbo. Caso contrário, ativar quadros jumbo realmente reduz o desempenho da rede substancialmente.

Configurar um SVM para iSCSI

Para configurar uma máquina virtual de storage (SVM) para iSCSI, você deve criar LIFs para o SVM e atribuir o protocolo iSCSI a esses LIFs.

Sobre esta tarefa

Você precisa de, no mínimo, um iSCSI LIF por nó para cada SVM que forneça dados com o protocolo iSCSI. Para redundância, você deve criar pelo menos duas LIFs por nó.

Exemplo 7. Passos

System Manager

Configurar uma VM de armazenamento para iSCSI com o Gestor de sistema ONTAP (9,7 e posterior).

Para configurar iSCSI em uma nova VM de armazenamento	Para configurar iSCSI em uma VM de armazenamento existente
1. No System Manager, clique em **Storage > Storage VMs** e, em seguida, clique em **Add**. 2. Introduza um nome para a VM de armazenamento. 3. Selecione **iSCSI** para o **Protocolo de Acesso**. 4. Clique em **Enable iSCSI** (Ativar iSCSI) e introduza o endereço IP e a máscara de sub-rede para a interface de rede. Cada nó deve ter pelo menos duas interfaces de rede. 5. Clique em **Salvar**.	1. No System Manager, clique em **Storage > Storage VMs**. 2. Clique na VM de armazenamento que você deseja configurar. 3. Clique no separador **Definições** e, em seguida, clique em junto ao protocolo iSCSI. 4. Clique em **Enable iSCSI** (Ativar iSCSI) e introduza o endereço IP e a máscara de sub-rede para a interface de rede. Cada nó deve ter pelo menos duas interfaces de rede. 5. Clique em **Salvar**.

CLI

Configure uma VM de armazenamento para iSCSI com a CLI do ONTAP.

1. Ative os SVMs para ouvir tráfego iSCSI:

   ```
   vserver iscsi create -vserver vserver_name -target-alias vserver_name
   ```

2. Crie um LIF para os SVMs em cada nó a ser usado para iSCSI:
   - Para o ONTAP 9.6 e posterior:

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol iscsi -service-policy default-data-iscsi -home-node node_name
     -home-port port_name -address ip_address -netmask netmask
     ```

   - Para o ONTAP 9.5 e versões anteriores:

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol iscsi -home-node node_name -home-port port_name -address
     ip_address -netmask netmask
     ```

3. Verifique se você configurou seus LIFs corretamente:

   ```
   network interface show -vserver vserver_name
   ```

4. Verifique se o iSCSI está ativo e em execução e o IQN de destino para esse SVM:

   ```
   vserver iscsi show –vserver vserver_name
   ```

5. A partir do seu host, crie sessões iSCSI para seus LIFs.

Informações relacionadas

"Relatório técnico da NetApp 4080: Práticas recomendadas para SAN moderna"

Defina um método de política de segurança para um iniciador

Você pode definir uma lista de iniciadores e seus métodos de autenticação. Você também pode modificar o método de autenticação padrão que se aplica a iniciadores que não possuem um método de autenticação definido pelo usuário.

Sobre esta tarefa

Você pode gerar senhas exclusivas usando algoritmos de política de segurança no produto ou especificar manualmente as senhas que deseja usar.

Nem todos os iniciadores suportam senhas secretas CHAP hexadecimais.

Passos

1. Use o `vserver iscsi security create` comando para criar um método de diretiva de segurança para um iniciador.

   ```
   vserver iscsi security create -vserver vs2 -initiator iqn.1991-
   05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name
   bob2
   ```

2. Siga os comandos do ecrã para adicionar as palavras-passe.

   Cria um método de política de segurança para o iniciador iqn.1991-05.com.microsoft:host1 com nomes de usuário CHAP de entrada e saída e senhas.

Informações relacionadas

- Como a autenticação iSCSI funciona
- Autenticação CHAP

Excluir um serviço iSCSI de um SVM

Você pode excluir um serviço iSCSI de uma máquina virtual de armazenamento (SVM) se não for mais necessário.

O que você vai precisar

O status de administração do serviço iSCSI deve estar no estado "próprio" antes de poder excluir um serviço iSCSI. Você pode mover o status de administração para baixo com o `vserver iscsi modify` comando.

Passos

1. Use o `vserver iscsi modify` comando para parar a e/S para o LUN.

   ```
   vserver iscsi modify -vserver vs1 -status-admin down
   ```

2. Use o `vserver iscsi delete` comando para remover o serviço iscsi do SVM.

   ```
   vserver iscsi delete -vserver vs_1
   ```

3. Use o `vserver iscsi show command` para verificar se você excluiu o serviço iSCSI do SVM.

```
vserver iscsi show -vserver vs1
```

Obtenha mais detalhes em recuperações de erros de sessão iSCSI

Aumentar o nível de recuperação de erros de sessão iSCSI permite-lhe receber informações mais detalhadas sobre recuperações de erros iSCSI. O uso de um nível de recuperação de erros mais alto pode causar uma redução menor no desempenho da sessão iSCSI.

Sobre esta tarefa

Por padrão, o ONTAP é configurado para usar o nível de recuperação de erro 0 para sessões iSCSI. Se você estiver usando um iniciador que foi qualificado para o nível de recuperação de erros 1 ou 2, você pode optar por aumentar o nível de recuperação de erros. O nível de recuperação de erro de sessão modificado afeta apenas as sessões recém-criadas e não afeta as sessões existentes.

A partir do ONTAP 9.4, a `max-error-recovery-level` opção não é suportada `iscsi show` nos comandos e. `iscsi modify`

Passos

1. Entrar no modo avançado:

```
set -privilege advanced
```

2. Verifique a configuração atual usando o `iscsi show` comando.

```
iscsi show -vserver vs3 -fields max-error-recovery-level
```

```
vserver max-error-recovery-level
------- ------------------------
vs3     0
```

3. Altere o nível de recuperação de erros usando o `iscsi modify` comando.

```
iscsi modify -vserver vs3 -max-error-recovery-level 2
```

Registre o SVM em um servidor iSNS

Você pode usar o `vserver iscsi isns` comando para configurar a máquina virtual de armazenamento (SVM) para se Registrar em um servidor iSNS.

Sobre esta tarefa

O `vserver iscsi isns create` comando configura o SVM para se Registrar no servidor iSNS. O SVM não fornece comandos que permitem configurar ou gerenciar o servidor iSNS. Para gerenciar o servidor iSNS, você pode usar as ferramentas de administração do servidor ou a interface fornecida pelo fornecedor para o servidor iSNS.

Passos

1. No servidor iSNS, certifique-se de que o serviço iSNS está ativo e disponível para serviço.
2. Crie o LIF de gerenciamento de SVM em uma porta de dados:

   ```
   network interface create -vserver SVM_name -lif lif_name -role data -data
   -protocol none -home-node home_node_name -home-port home_port -address
   IP_address -netmask network_mask
   ```

3. Crie um serviço iSCSI no SVM se ainda não existir um:

   ```
   vserver iscsi create -vserver SVM_name
   ```

4. Verifique se o serviço iSCSI foi criado com sucesso:

   ```
   iscsi show -vserver SVM_name
   ```

5. Verifique se existe uma rota padrão para o SVM:

   ```
   network route show -vserver SVM_name
   ```

6. Se uma rota padrão não existir para o SVM, crie uma rota padrão:

   ```
   network route create -vserver SVM_name -destination destination -gateway
   gateway
   ```

7. Configure o SVM para se Registrar no serviço iSNS:

   ```
   vserver iscsi isns create -vserver SVM_name -address IP_address
   ```

   As famílias de endereços IPv4 e IPv6 são apoiadas. A família de endereços do servidor iSNS deve ser a mesma do LIF de gerenciamento do SVM.

   Por exemplo, você não pode conetar um LIF de gerenciamento de SVM com um endereço IPv4 a um servidor iSNS com um endereço IPv6.

8. Verifique se o serviço iSNS está em execução:

   ```
   vserver iscsi isns show -vserver SVM_name
   ```

9. Se o serviço iSNS não estiver em execução, inicie-o:

   ```
   vserver iscsi isns start -vserver SVM_name
   ```

Resolva mensagens de erro iSCSI no sistema de armazenamento

Existem várias mensagens de erro comuns relacionadas ao iSCSI que podem ser visualizadas com o `event log show` comando. Você precisa saber o que essas mensagens significam e o que você pode fazer para resolver os problemas que elas identificam.

A tabela a seguir contém as mensagens de erro mais comuns e instruções para resolvê-las:

Mensagem	Explicação	O que fazer
`ISCSI: network interface identifier disabled for use; incoming connection discarded`	O serviço iSCSI não está ativado na interface.	Pode utilizar o `iscsi interface enable` comando para ativar o serviço iSCSI na interface. Por exemplo: `iscsi interface enable -vserver vs1 -lif lif1`
`ISCSI: Authentication failed for initiator nodename`	O CHAP não está configurado corretamente para o iniciador especificado.	Deve verificar as definições CHAP; não pode utilizar o mesmo nome de utilizador e palavra-passe para as definições de entrada e saída no sistema de armazenamento: • As credenciais de entrada no sistema de storage devem corresponder às credenciais de saída no iniciador. • As credenciais de saída no sistema de storage devem corresponder às credenciais de entrada no iniciador.

Ativar ou desativar o failover automático de iSCSI LIF

Depois de atualizar para o ONTAP 9.11,1 ou posterior, deverá ativar manualmente o failover automático de LIF em todas as LIFs iSCSI criadas no ONTAP 9.10,1 ou anterior.

A partir do ONTAP 9.11,1, você pode ativar o failover automático de LIF para LIFs iSCSI em plataformas all-flash de storage SAN. Se ocorrer um failover de armazenamento, o iSCSI LIF é migrado automaticamente de seu nó ou porta inicial para o nó ou porta do parceiro de HA e, em seguida, volta assim que o failover for concluído. Ou, se a porta para iSCSI LIF não for saudável, o LIF é migrado automaticamente para uma porta saudável em seu nó inicial atual e, em seguida, de volta para sua porta original quando a porta estiver funcionando novamente. O permite que os workloads SAN executados no iSCSI retomem o serviço de e/S mais rapidamente após a ocorrência de um failover.

No ONTAP 9.11,1 e posterior, por padrão, os LIFs iSCSI recém-criados são ativados para failover automático de LIF se uma das seguintes condições for verdadeira:

- Não há iSCSI LIFs no SVM
- Todas as LIFs iSCSI na SVM são ativadas para failover automático de LIF

Ativar failover automático de LIF iSCSI

Por padrão, LIFs iSCSI criadas no ONTAP 9.10,1 e anteriores não são ativadas para failover automático de LIF. Se houver iSCSI LIFs na SVM que não estejam habilitadas para failover automático de LIF, seus LIFs recém-criados também não serão ativados para failover automático de LIF. Se o failover automático de LIF não estiver ativado e houver um evento de failover, seus iSCSI LIFs não serão migrados.

Saiba mais "Failover de LIF e giveback"sobre o .

Passo

1. Ativar failover automático para um iSCSI LIF:

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy sfo-partner-only -auto-revert true
```

Para atualizar todas as LIFs iSCSI na SVM, use `-lif*` em vez `lif` de .

Desativar o failover automático de LIF iSCSI

Se você ativou anteriormente o failover automático de LIF iSCSI em LIFs iSCSI criados no ONTAP 9.10,1 ou anterior, você tem a opção de desativá-lo.

Passo

1. Desativar failover automático para um iSCSI LIF:

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy disabled -auto-revert false
```

Para atualizar todas as LIFs iSCSI na SVM, use `-lif*` em vez `lif` de .

Informações relacionadas

- "Crie um LIF"
- Manualmente "Migração de um LIF"
- Manualmente "Reverter um LIF para sua porta inicial"
- "Configure as configurações de failover em um LIF"

Gerenciar o protocolo FC

Configurar um SVM para FC

Para configurar uma máquina virtual de storage (SVM) para FC, você deve criar LIFs para o SVM e atribuir o protocolo FC a esses LIFs.

Antes de começar

Você deve ter uma licença FC ("Incluído no ONTAP One") e ela deve estar habilitada. Se a licença FC não estiver ativada, os LIFs e SVMs parecerão estar online, mas o status operacional será `down`. O serviço FC precisa estar habilitado para que seus LIFs e SVMs estejam operacionais. Você deve usar o zoneamento de iniciador único para todos os LIFs FC no SVM para hospedar os iniciadores.

Sobre esta tarefa

O NetApp dá suporte a pelo menos um FC LIF por nó para cada SVM, fornecendo dados com o protocolo FC. É necessário usar duas LIFs por nó e duas malhas, com um LIF por nó anexado. Isso fornece redundância na camada de nó e na malha.

Exemplo 8. Passos

System Manager

Configurar uma VM de armazenamento para iSCSI com o Gestor de sistema ONTAP (9,7 e posterior).

Para configurar o FC em uma nova VM de storage	Para configurar o FC em uma VM de storage existente
1. No System Manager, clique em **Storage > Storage VMs** e, em seguida, clique em **Add**. 2. Introduza um nome para a VM de armazenamento. 3. Selecione **FC** para o **Protocolo de Acesso**. 4. Clique em **Ativar FC**. As portas FC são atribuídas automaticamente. 5. Clique em **Salvar**.	1. No System Manager, clique em **Storage > Storage VMs**. 2. Clique na VM de armazenamento que você deseja configurar. 3. Clique na guia **Configurações** e, em seguida, clique ⚙ ao lado do protocolo FC. 4. Clique em **Enable FC** (Ativar FC) e introduza o endereço IP e a máscara de sub-rede para a interface de rede. As portas FC são atribuídas automaticamente. 5. Clique em **Salvar**.

CLI

1. Habilite o serviço FC na SVM:

   ```
   vserver fcp create -vserver vserver_name -status-admin up
   ```

2. Crie duas LIFs para as SVMs em cada nó que fornece FC:
   - Para o ONTAP 9.6 e posterior:

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol fcp -service-policy default-data-fcp -home-node node_name
     -home-port port_name -address ip_address -netmask netmask -status-admin
     up
     ```

   - Para o ONTAP 9.5 e versões anteriores:

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol fcp -home-node node_name -home-port port
     ```

3. Verifique se seus LIFs foram criados e se o status operacional deles é `online`:

   ```
   network interface show -vserver vserver_name lif_name
   ```

Informações relacionadas

"Suporte à NetApp"

"Ferramenta de Matriz de interoperabilidade do NetApp"

Considerações para LIFs em ambientes SAN de cluster

Excluir um serviço FC de um SVM

Você pode excluir um serviço FC de uma máquina virtual de storage (SVM) se não for mais necessário.

O que você vai precisar

O status de administração deve ser "próprio" antes de excluir um serviço FC de um SVM. Você pode definir o status de administração para baixo com o `vserver fcp modify` comando ou o `vserver fcp stop` comando.

Passos

1. Use o `vserver fcp stop` comando para parar a e/S para o LUN.

   ```
   vserver fcp stop -vserver vs_1
   ```

2. Use o `vserver fcp delete` comando para remover o serviço da SVM.

   ```
   vserver fcp delete -vserver vs_1
   ```

3. Use o `vserver fcp show` para verificar se você excluiu o serviço FC do SVM:

   ```
   vserver fcp show -vserver vs_1
   ```

Configurações de MTU recomendadas para quadros jumbo FCoE

Para Fibre Channel over Ethernet (FCoE), os quadros jumbo para a parte do adaptador Ethernet da CNA devem ser configurados em 9000 MTU. Os frames grandes para a parte do adaptador FCoE da CNA devem ser configurados com mais de 1500 MTU. Apenas configure quadros jumbo se o iniciador, o alvo e todos os switches intervenientes suportarem e estiverem configurados para quadros jumbo.

Gerenciar o protocolo NVMe

Inicie o serviço NVMe em uma SVM

Antes de usar o protocolo NVMe na máquina virtual de storage (SVM), é necessário iniciar o serviço NVMe no SVM.

Antes de começar

O NVMe deve ser permitido como protocolo no seu sistema.

Os seguintes protocolos NVMe são compatíveis:

Protocolo	Começando com …	Permitido por…
TCP	ONTAP 9.10,1	Padrão
FCP	ONTAP 9,4	Padrão

Passos

1. Altere a configuração de privilégios para avançado:

   ```
   set -privilege advanced
   ```

2. Verifique se o NVMe é permitido como protocolo:

   ```
   vserver nvme show
   ```

3. Criar o serviço de protocolo NVMe:

   ```
   vserver nvme create
   ```

4. Inicie o serviço de protocolo NVMe na SVM:

   ```
   vserver nvme modify -status -admin up
   ```

Excluir o serviço NVMe de um SVM

Se necessário, você pode excluir o serviço NVMe da sua máquina virtual de storage (SVM).

Passos

1. Altere a configuração de privilégios para avançado:

   ```
   set -privilege advanced
   ```

2. Pare o serviço NVMe na SVM:

   ```
   vserver nvme modify -status -admin down
   ```

3. Exclua o serviço NVMe:

   ```
   vserver nvme delete
   ```

Redimensione um namespace

A partir do ONTAP 9.10,1, você pode usar a CLI do ONTAP para aumentar ou diminuir o tamanho de um namespace NVMe. Você pode usar o System Manager para aumentar o tamanho de um namespace NVMe.

Aumente o tamanho de um namespace

System Manager

1. Clique em **Storage > NVMe Namespaces**.
2. Passe o espaço de nomes que você deseja aumentar, clique em e, em seguida, clique em **Editar**.
3. Em **CAPACIDADE**, altere o tamanho do namespace.

CLI

1. Introduza o seguinte comando: `vserver nvme namespace modify -vserver SVM_name -path path –size new_size_of_namespace`

Diminua o tamanho de um namespace

Use a CLI do ONTAP para diminuir o tamanho de um namespace NVMe.

1. Altere a configuração de privilégios para avançado:

   ```
   set –privilege advanced
   ```

2. Diminua o tamanho do namespace:

   ```
   vserver nvme namespace modify -vserver SVM_name -path namespace_path -size new_size_of_namespace
   ```

Converta um namespace em um LUN

A partir do ONTAP 9.11,1, você pode usar a CLI do ONTAP para converter no local um namespace NVMe existente em um LUN.

Antes de começar

- Namespace NVMe especificado não deve ter nenhum mapa existente para um subsistema.
- O namespace não deve fazer parte de uma cópia Snapshot ou no lado de destino da relação do SnapMirror como namespace somente leitura.
- Como os namespaces NVMe só são compatíveis com plataformas específicas e placas de rede, esse recurso funciona apenas com hardware específico.

Passos

1. Digite o seguinte comando para converter um namespace NVMe em um LUN:

   ```
   lun convert-from-namespace -vserver -namespace-path
   ```

Configurar a autenticação na banda pelo NVMe

A partir do ONTAP 9.12,1, você pode usar a interface de linha de comando (CLI) do ONTAP para configurar a autenticação na banda (segura), bidirecional e unidirecional entre um host e uma controladora NVMe através dos protocolos NVMe/TCP e NVMe/FC usando a autenticação DH-HMAC-CHAP. A partir do ONTAP 9.14,1, a autenticação na banda pode ser configurada no Gerenciador do sistema.

Para configurar a autenticação na banda, cada host ou controlador deve estar associado a uma chave DH-HMAC-CHAP, que é uma combinação do NQN do host ou controlador NVMe e um segredo de autenticação configurado pelo administrador. Para que um host ou controlador NVMe autentique seu peer, ele precisa saber a chave associada ao mesmo.

Na autenticação unidirecional, uma chave secreta é configurada para o host, mas não para o controlador. Na autenticação bidirecional, uma chave secreta é configurada para o host e para o controlador.

Sha-256 é a função hash padrão e 2048-bit é o grupo DH padrão.

System Manager

A partir do ONTAP 9.14,1, é possível usar o Gerenciador do sistema para configurar a autenticação na banda ao criar ou atualizar um subsistema NVMe, criar ou clonar espaços de nomes NVMe ou adicionar grupos de consistência com novos namespaces NVMe.

Passos

1. No System Manager, clique em **hosts > NVMe Subsystem** e, em seguida, clique em **Add**.
2. Adicione o nome do subsistema NVMe e selecione a VM de storage e o sistema operacional de host.
3. Introduza o NQN do anfitrião.
4. Selecione **Use in-band Authentication** ao lado do Host NQN.
5. Forneça o segredo do host e o segredo do controlador.

   A chave DH-HMAC-CHAP é uma combinação do NQN do host ou controlador NVMe e um segredo de autenticação configurado pelo administrador.

6. Selecione a função hash preferida e o grupo DH para cada host.

   Se você não selecionar uma função hash e um grupo DH, SHA-256 é atribuído como a função hash padrão e 2048 bits é atribuído como o grupo DH padrão.

7. Opcionalmente, clique em **Add** e repita as etapas conforme necessário para adicionar mais host.
8. Clique em **Salvar**.
9. Para verificar se a autenticação na banda está ativada, clique em **System Manager > hosts > NVMe Subsystem > Grid > Peek view**.

   Um ícone de chave transparente ao lado do nome do host indica que o modo unidirecional está ativado. Uma tecla opaca ao lado do nome do host indica que o modo bidirecional está ativado.

CLI

Passos

1. Adicione a autenticação DH-HMAC-CHAP ao subsistema NVMe:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -dhchap-host-secret
<authentication_host_secret> -dhchap-controller-secret
<authentication_controller_secret> -dhchap-hash-function <sha-
256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
bit|8192-bit>
```

2. Verifique se o protocolo de autenticação DH-HMAC CHAP foi adicionado ao seu host:

```
vserver nvme subsystem host show
```

```
  [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
  [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
  [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

3. Verifique se a autenticação DH-HMAC CHAP foi executada durante a criação do controlador NVMe:

```
vserver nvme subsystem controller show
```

```
 [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
 [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
 [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

Desativar a autenticação na banda pelo NVMe

Se você configurou a autenticação na banda pelo NVMe usando DH-HMAC-CHAP, você pode optar por desativá-la a qualquer momento.

Se estiver a reverter do ONTAP 9.12,1 ou posterior para o ONTAP 9.12,0 ou anterior, tem de desativar a autenticação na banda antes de reverter. Se a autenticação na banda usando DH-HMAC-CHAP não estiver desativada, a reversão falhará.

Passos

1. Remova o host do subsistema para desativar a autenticação DH-HMAC-CHAP:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Verifique se o protocolo de autenticação DH-HMAC-CHAP foi removido do host:

```
vserver nvme subsystem host show
```

3. Adicione o host de volta ao subsistema sem autenticação:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Configurar o canal seguro TLS para NVMe/TCP

A partir do ONTAP 9.16,1, você pode configurar o canal seguro TLS para conexões NVMe/TCP. Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para adicionar um novo subsistema NVMe com TLS habilitado ou habilitar o TLS para um subsistema NVMe existente.

System Manager

A partir do ONTAP 9.16,1, você pode usar o Gerenciador de sistemas para configurar o TLS para conexões NVMe/TCP ao criar ou atualizar um subsistema NVMe, criar ou clonar espaços de nomes NVMe ou adicionar grupos de consistência com novos namespaces NVMe.

Passos

1. No System Manager, clique em **hosts > NVMe Subsystem** e, em seguida, clique em **Add**.
2. Adicione o nome do subsistema NVMe e selecione a VM de storage e o sistema operacional de host.
3. Introduza o NQN do anfitrião.
4. Selecione **Require Transport Layer Security (TLS)** ao lado do NQN do host.
5. Forneça a chave pré-compartilhada (PSK).
6. Clique em **Salvar**.
7. Para verificar se o canal seguro TLS está ativado, selecione **System Manager > hosts > NVMe Subsystem > Grid > Peek view**.

CLI

Passos

1. Adicione um host de subsistema NVMe compatível com o canal seguro TLS. Você pode fornecer uma chave pré-compartilhada (PSK) usando o `tls-configured-psk` argumento, ou usar um PSK gerado usando o `tls-generated-psk` argumento:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> {-tls-configured-psk <key_text> |
-tls-generated-psk true}
```

2. Verifique se o host do subsistema NVMe está configurado para o canal seguro TLS. Opcionalmente, você pode usar o `tls-key-type` argumento para exibir somente os hosts que estão usando esse tipo de chave:

```
vserver nvme subsystem host show -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-key-type
{none|configured|generated}
```

3. Verifique se a controladora de host do subsistema NVMe está configurada para o canal seguro TLS. Opcionalmente, você pode usar qualquer um dos `tls-key-type` argumentos , `tls-identity` ou `tls-cipher` para exibir somente os controladores que têm esses atributos TLS:

```
vserver nvme subsystem controller show -vserver <svm_name>
-subsystem <subsystem> -host-nqn <host_nqn> -tls-key-type
{none|configured|generated} -tls-identity <text> -tls-cipher
{none|TLS_AES_128_GCM_SHA256|TLS_AES_256_GCM_SHA384}
```

Saiba mais

Visite as páginas do manual do ONTAP para estes comandos:

- "adicionar o host do subsistema nvme do svm"
- "mostra o host do subsistema nvme do svm"
- "o controlador do subsistema do svm nvme mostra"

Desative o canal seguro TLS para NVMe/TCP

A partir do ONTAP 9.16,1, você pode configurar o canal seguro TLS para conexões NVMe/TCP. Se você configurou o canal seguro TLS para conexões NVMe/TCP, pode optar por desativá-lo a qualquer momento.

Passos

1. Remova o host do subsistema para desativar o canal seguro TLS:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Verifique se o canal seguro TLS é removido do host:

```
vserver nvme subsystem host show
```

3. Adicione o host de volta ao subsistema sem o canal seguro TLS:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Saiba mais

Visite as páginas do manual do ONTAP para estes comandos:

- "adicionar o host do subsistema nvme do svm"
- "remoção do host do subsistema nvme do svm"
- "mostra o host do subsistema nvme do svm"

Alterar a prioridade do host NVMe

A partir do ONTAP 9.14,1, você pode configurar o subsistema NVMe para priorizar a alocação de recursos para hosts específicos. Por padrão, quando um host é adicionado ao subsistema, é atribuída uma prioridade regular. Os hosts atribuídos a uma alta prioridade são alocadas contagens de filas de e/S maiores e profundidades de filas.

Você pode usar a interface de linha de comando (CLI) do ONTAP para alterar manualmente a prioridade padrão de regular para alta. Para alterar a prioridade atribuída a um host, você deve remover o host do

subsistema e adicioná-lo de volta.

Passos

1. Verifique se a prioridade do host está definida como regular:

```
vserver nvme show-host-priority
```

2. Remova o host do subsistema:

```
vserver nvme subsystem host remove –vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

3. Verifique se o host foi removido do subsistema:

```
vserver nvme subsystem host show
```

4. Adicione o host de volta ao subsistema com alta prioridade:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
-priority high
```

Gerenciar a detecção automatizada de host das controladoras NVMe/TCP

A partir do ONTAP 9.14,1, a descoberta de hosts de controladoras usando o protocolo NVMe/TCP é automatizada por padrão em malhas baseadas em IP.

Habilitar a detecção automatizada de host das controladoras NVMe/TCP

Se você desativou anteriormente a descoberta automatizada de host, mas suas necessidades foram alteradas, você pode reativá-la.

Passos

1. Entrar no modo de privilégio avançado:

```
set -privilege advanced
```

2. Ativar a deteção automatizada:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled true
```

3. Verifique se a detecção automatizada de controladores NVMe/TCP está ativada.

```
vserver nvme show
```

Desativar a descoberta automatizada de host das controladoras NVMe/TCP

Se você não precisar que controladores NVMe/TCP sejam detetados automaticamente pelo host e detetar tráfego multicast indesejado na rede, desative essa funcionalidade.

Passos

1. Entrar no modo de privilégio avançado:

```
set -privilege advanced
```

2. Desativar a deteção automatizada:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled false
```

3. Verifique se a detecção automatizada de controladores NVMe/TCP está desativada.

```
vserver nvme show
```

Desative o identificador da máquina virtual do host NVMe

A partir do ONTAP 9.14,1, por padrão, o ONTAP oferece suporte à capacidade de hosts NVMe/FC identificarem máquinas virtuais por um identificador exclusivo e de hosts NVMe/FC monitorarem a utilização de recursos da máquina virtual. Isso aprimora a geração de relatórios e a solução de problemas no lado do host.

Você pode usar o bootarg para desativar essa funcionalidade.

Passo

1. Desative o identificador da máquina virtual:

```
bootargs set fct_sli_appid_off <port>, <port>
```

O exemplo a seguir desativa o VMID na porta 0g e na porta 0i.

```
bootargs set fct_sli_appid_off 0g,0i

fct_sli_appid_off == 0g,0i
```

Gerenciar sistemas com adaptadores FC

Gerenciar sistemas com adaptadores FC

Os comandos estão disponíveis para gerenciar adaptadores FC integrados e placas adaptadoras FC. Esses comandos podem ser usados para configurar o modo do adaptador, exibir informações do adaptador e alterar a velocidade.

A maioria dos sistemas de storage tem adaptadores FC integrados que podem ser configurados como iniciadores ou destinos. Você também pode usar placas de adaptador FC configuradas como iniciadores ou destinos. Os iniciadores se conetam aos compartimentos de disco back-end e, possivelmente, a matrizes de armazenamento estranho (FlexArray). Os destinos se conetam apenas aos switches FC. Ambas as portas HBA de destino FC e a velocidade da porta do switch devem ser definidas para o mesmo valor e não devem ser definidas para auto.

Informações relacionadas

"Configuração SAN"

Comandos para gerenciar adaptadores FC

Você pode usar comandos FC para gerenciar adaptadores de destino FC, adaptadores iniciadores FC e adaptadores FC integrados para o controlador de storage. Os mesmos comandos são usados para gerenciar adaptadores FC para o protocolo FC e o protocolo FC-NVMe.

Os comandos do adaptador do iniciador FC funcionam apenas no nível do nó. Você deve usar o `run -node node_name` comando antes de usar os comandos do adaptador do iniciador FC.

Comandos para gerenciar adaptadores de destino FC

Se você quiser…	Use este comando…
Exibir as informações do adaptador FC em um nó	`network fcp adapter show`
Modifique os parâmetros do adaptador de destino FC	`network fcp adapter modify`
Apresentar informações de tráfego do protocolo FC	`run -node node_name sysstat -f`
Apresentar durante quanto tempo o protocolo FC foi executado	`run -node node_name uptime`

Se você quiser…	Use este comando…
Exibir configuração e status do adaptador	`run -node node_name sysconfig -v adapter`
Verifique quais placas de expansão estão instaladas e se existem erros de configuração	`run -node node_name sysconfig -ac`
Exibir uma página de manual para um comando	`man command_name`

Comandos para gerenciar adaptadores de iniciador FC

Se você quiser…	Use este comando…
Exibir informações para todos os iniciadores e seus adaptadores em um nó	`run -node node_name storage show adapter`
Exibir configuração e status do adaptador	`run -node node_name sysconfig -v adapter`
Verifique quais placas de expansão estão instaladas e se existem erros de configuração	`run -node node_name sysconfig -ac`

Comandos para gerenciar adaptadores FC integrados

Se você quiser…	Use este comando…
Exibir o status das portas FC integradas	`run -node node_name system hardware unified-connect show`

Configurar adaptadores FC

Cada porta FC integrada pode ser configurada individualmente como iniciador ou destino. As portas em certos adaptadores FC também podem ser configuradas individualmente como uma porta de destino ou uma porta de iniciador, assim como as portas FC integradas. Uma lista de adaptadores que podem ser configurados para o modo de destino está disponível no "NetApp Hardware Universe".

O modo de destino é usado para conetar as portas aos iniciadores FC. O modo iniciador é usado para conetar as portas a unidades de fita, bibliotecas de fita ou armazenamento de terceiros com virtualização FlexArray ou importação de LUN estrangeiro (FLI).

As mesmas etapas são usadas na configuração de adaptadores FC para o protocolo FC e para o protocolo FC-NVMe. No entanto, apenas certos adaptadores FC são compatíveis com FC-NVMe. Consulte "NetApp Hardware Universe" a para obter uma lista de adaptadores compatíveis com o protocolo FC-NVMe.

Configurar adaptadores FC para o modo de destino

Passos

1. Coloque o adaptador offline:

   `node run -node node_name storage disable adapter adapter_name`

   Se o adaptador não ficar offline, você também pode remover o cabo da porta apropriada do adaptador no sistema.

2. Altere o adaptador do iniciador para o destino:

   `system hardware unified-connect modify -t target -node node_name adapter adapter_name`

3. Reinicie o nó que hospeda o adaptador que você alterou.
4. Verifique se a porta de destino tem a configuração correta:

   `network fcp adapter show -node node_name`

5. Coloque o adaptador online:

   `network fcp adapter modify -node node_name -adapter adapter_port -state up`

Configurar adaptadores FC para o modo iniciador

O que você vai precisar

- Os LIFs no adaptador devem ser removidos de quaisquer conjuntos de portas dos quais sejam membros.
- Todos os LIF de todas as máquinas virtuais de armazenamento (SVM) que usam a porta física a ser modificada devem ser migrados ou destruídos antes de alterar a personalidade da porta física de destino para iniciador.

O NVMe/FC oferece suporte ao modo iniciador.

Passos

1. Remova todas as LIFs do adaptador:

   `network interface delete -vserver SVM_name -lif LIF_name,LIF_name`

2. Coloque o adaptador offline:

   `network fcp adapter modify -node node_name -adapter adapter_port -status-admin down`

   Se o adaptador não ficar offline, você também pode remover o cabo da porta apropriada do adaptador no sistema.

3. Altere o adaptador de destino para iniciador:

   `system hardware unified-connect modify -t initiator adapter_port`

4. Reinicie o nó que hospeda o adaptador que você alterou.

5. Verifique se as portas FC estão configuradas no estado correto para sua configuração:

   `system hardware unified-connect show`

6. Coloque o adaptador novamente online:

   `node run -node node_name storage enable adapter adapter_port`

Ver as definições do adaptador

Você pode usar comandos específicos para exibir informações sobre seus adaptadores FC/UTA.

Adaptador de destino FC

Passo

1. Use o `network fcp adapter show` comando para exibir informações do adaptador: `network fcp adapter show -instance -node node1 -adapter 0a`

   A saída exibe informações de configuração do sistema e informações do adaptador para cada slot usado.

Adaptador de destino unificado (UTA) X1143A-R6

Passos

1. Inicialize seu controlador sem os cabos conetados.
2. Execute o `system hardware unified-connect show` comando para ver a configuração da porta e os módulos.
3. Visualize as informações da porta antes de configurar o CNA e as portas.

Altere a porta UTA2 do modo CNA para o modo FC

Você deve alterar a porta UTA2 do modo de adaptador de rede convergente (CNA) para o modo Fibre Channel (FC) para suportar o iniciador FC e o modo de destino FC. Você deve alterar a personalidade do modo CNA para o modo FC quando precisar alterar o meio físico que coneta a porta à sua rede.

Passos

1. Coloque o adaptador offline:

   `network fcp adapter modify -node node_name -adapter adapter_name -status-admin down`

2. Alterar o modo de porta:

   `ucadmin modify -node node_name -adapter adapter_name -mode fcp`

3. Reinicie o nó e, em seguida, coloque o adaptador online:

   `network fcp adapter modify -node node_name -adapter adapter_name -status-admin up`

4. Notifique seu administrador ou gerenciador de VIF para excluir ou remover a porta, conforme aplicável:

   - Se a porta for usada como uma porta inicial de um LIF, for um membro de um grupo de interfaces (ifgrp) ou hosts VLANs, então um administrador deve fazer o seguinte:
     i. Mova os LIFs, remova a porta do ifgrp ou exclua as VLANs, respetivamente.
     ii. Exclua manualmente a porta executando o `network port delete` comando.

     Se o `network port delete` comando falhar, o administrador deve resolver os erros e, em seguida, executar o comando novamente.

   - Se a porta não for usada como porta inicial de um LIF, não for membro de um ifgrp e não hospedar VLANs, o gerenciador de VIF deve remover a porta de seus Registros no momento da reinicialização.

     Se o gerenciador de VIF não remover a porta, o administrador deve removê-la manualmente após a reinicialização usando o `network port delete` comando.

```
net-f8040-34::> network port show

    Node: net-f8040-34-01
                                                      Speed(Mbps) Health
    Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
    --------- ------------ ---------------- ---- ---- -----------
--------
    ...
    e0i       Default      Default          down 1500  auto/10     -
    e0f       Default      Default          down 1500  auto/10     -
    ...

    net-f8040-34::> ucadmin show
                               Current  Current    Pending  Pending
Admin
    Node            Adapter   Mode     Type       Mode     Type
Status
    ------------    -------   -------  ---------  -------  ---------
-----------
    net-f8040-34-01   0e       cna      target     -        -
offline
    net-f8040-34-01   0f       cna      target     -        -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0
```

```
    net-f8040-34::> network interface show -fields home-port, curr-port

    vserver lif                   home-port curr-port
    ------- --------------------- --------- ---------
    Cluster net-f8040-34-01_clus1 e0a       e0a
    Cluster net-f8040-34-01_clus2 e0b       e0b
    Cluster net-f8040-34-01_clus3 e0c       e0c
    Cluster net-f8040-34-01_clus4 e0d       e0d
    net-f8040-34
            cluster_mgmt          e0M       e0M
    net-f8040-34
            m                     e0e       e0i
    net-f8040-34
            net-f8040-34-01_mgmt1 e0M       e0M
    7 entries were displayed.

    net-f8040-34::> ucadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed to
fc.
    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

    net-f8040-34::> reboot local
      (system node reboot)

    Warning: Are you sure you want to reboot node "net-f8040-34-01"?
    {y|n}: y
```

5. Verifique se você tem o SFP correto instalado:

   `network fcp adapter show -instance -node -adapter`

   Para CNA, você deve usar um SFP Ethernet 10Gb. Para FC, você deve usar um SFP de 8 GB ou um SFP de 16 GB antes de alterar a configuração no nó.

Altere os módulos óticos do adaptador de destino CNA/UTA2

Você deve alterar os módulos óticos no adaptador de destino unificado (CNA/UTA2) para suportar o modo de personalidade que você selecionou para o adaptador.

Passos

1. Verifique o SFP atual usado na placa. Em seguida, substitua o SFP atual pelo SFP apropriado para a personalidade preferida (FC ou CNA).
2. Remova os módulos óticos atuais do adaptador X1143A-R6.

3. Insira os módulos corretos para a ótica do seu modo de personalidade (FC ou CNA) preferido.
4. Verifique se você tem o SFP correto instalado:

   `network fcp adapter show -instance -node -adapter`

   Módulos SFP suportados e cabos de cobre (Twinax) da marca Cisco estão listados no *Hardware Universe*.

Informações relacionadas

"NetApp Hardware Universe"

Configurações de porta suportadas para adaptadores X1143A-R6

O modo de destino FC é a configuração padrão para portas de adaptador X1143A-R6. No entanto, as portas desse adaptador podem ser configuradas como portas Ethernet e FCoE de 10 GB ou como portas FC de 16 GB.

Quando configurados para Ethernet e FCoE, os adaptadores X1143A-R6 suportam NIC concorrente e tráfego de destino FCoE na mesma porta de 10 GBE. Quando configurado para FC, cada par de duas portas que compartilha o mesmo ASIC pode ser configurado individualmente para o modo de iniciador FC ou destino. Isso significa que um único adaptador X1143A-R6 pode oferecer suporte ao modo de destino FC em um par de duas portas e no modo iniciador FC em outro par de duas portas.

Informações relacionadas

"NetApp Hardware Universe"

"Configuração SAN"

Configure as portas

Para configurar o adaptador de destino unificado (X1143A-R6), você deve configurar as duas portas adjacentes no mesmo chip no mesmo modo de personalidade.

Passos

1. Configure as portas conforme necessário para Fibre Channel (FC) ou adaptador de rede convergente (CNA) usando o `system node hardware unified-connect modify` comando.
2. Conete os cabos apropriados para FC ou Ethernet de 10 GB.
3. Verifique se você tem o SFP correto instalado:

   `network fcp adapter show -instance -node -adapter`

   Para CNA, você deve usar um SFP Ethernet 10Gb. Para FC, você deve usar um SFP de 8 GB ou um SFP de 16 GB, com base na malha FC conetada.

Evite a perda de conetividade ao usar o adaptador X1133A-R6

Você pode evitar a perda de conetividade durante uma falha de porta configurando o sistema com caminhos redundantes para separar HBAs X1133A-R6.

O HBA X1133A-R6 é um adaptador FC de 4 portas e 16 GB que consiste em dois pares de 2 portas. O adaptador X1133A-R6 pode ser configurado como modo de destino ou modo de iniciador. Cada par de 2

portas é suportado por um único ASIC (por exemplo, porta 1 e porta 2 no ASIC 1 e porta 3 e porta 4 no ASIC 2). Ambas as portas em um único ASIC devem ser configuradas para operar no mesmo modo, seja no modo de destino ou no modo de iniciador. Se ocorrer um erro com o ASIC que suporta um par, ambas as portas do par ficam offline.

Para evitar essa perda de conetividade, configure o sistema com caminhos redundantes para separar HBAs X1133A-R6 ou com caminhos redundantes para portas compatíveis com ASICs diferentes no HBA.

Gerenciar LIFs para todos os protocolos SAN

Gerenciar LIFs para todos os protocolos SAN

Os iniciadores devem usar o Multipath I/o (MPIO) e o Asymmetric Logical Unit Access (ALUA) para capacidade de failover para clusters em um ambiente SAN. Se um nó falhar, os LIFs não migram nem assumem os endereços IP do nó do parceiro com falha. Em vez disso, o software MPIO, usando ALUA no host, é responsável por selecionar os caminhos apropriados para o acesso LUN por meio de LIFs.

É necessário criar um ou mais caminhos iSCSI a partir de cada nó em um par de HA, usando interfaces lógicas (LIFs) para permitir acesso a LUNs atendidas pelo par de HA. Você deve configurar um LIF de gerenciamento para cada máquina virtual de storage (SVM) que suporte SAN.

A conexão direta ou o uso de switches Ethernet são suportados para conetividade. Você deve criar LIFs para ambos os tipos de conetividade.

- Você deve configurar um LIF de gerenciamento para cada máquina virtual de storage (SVM) que suporte SAN. Você pode configurar duas LIFs por nó, uma para cada malha que está sendo usada com FC e para separar redes Ethernet para iSCSI.

Após a criação dos LIFs, eles podem ser removidos de conjuntos de portas, movidos para nós diferentes dentro de uma máquina virtual de storage (SVM) e excluídos.

Informações relacionadas

- "Configure a visão geral dos LIFs"
- "Crie um LIF"

Configurar um NVMe LIF

Certos requisitos devem ser atendidos ao configurar as LIFs do NVMe.

Antes de começar

O NVMe precisa ser compatível com o adaptador FC no qual você cria o LIF. Os adaptadores suportados estão listados em "Hardware Universe".

Sobre esta tarefa

A partir do ONTAP 9.12,1 e posterior, é possível configurar duas LIFs NVMe por nó em um máximo de 12 nós. No ONTAP 9.11,1 e versões anteriores, é possível configurar duas LIFs NVMe por nó no máximo dois nós.

As regras a seguir se aplicam ao criar um LIF NVMe:

- O NVMe pode ser o único protocolo de dados em LIFs de dados.

- Você deve configurar um LIF de gerenciamento para cada SVM compatível com SAN.
- Para o ONTAP 9.5 e posterior, você precisa configurar um LIF NVMe no nó que contém o namespace e o parceiro de HA do nó.
- Apenas para o ONTAP 9.4:
  - Os LIFs e namespaces NVMe devem ser hospedados no mesmo nó.
  - Somente um LIF de dados NVMe pode ser configurado por SVM.

Passos

1. Crie o LIF:

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>
-home-port <home_port>
```

NVMe/TCP está disponível a partir do ONTAP 9.10,1 e posterior.

2. Verifique se o LIF foi criado:

```
network interface show -vserver <SVM_name>
```

Após a criação, os LIFs NVMe/TCP escutam a descoberta na porta 8009.

O que saber antes de mover um SAN LIF

Você só precisa executar um movimento de LIF se estiver alterando o conteúdo do cluster, por exemplo, adicionando nós ao cluster ou excluindo nós do cluster. Se você executar um movimento de LIF, não será necessário rezonear sua malha FC ou criar novas sessões iSCSI entre os hosts anexados do cluster e a nova interface de destino.

Você não pode mover um SAN LIF usando o `network interface move` comando. O movimento DE SAN LIF deve ser realizado colocando o LIF offline, movendo o LIF para um nó ou porta inicial diferente e, em seguida, trazendo-o de volta on-line em sua nova localização. O Acesso lógico-Unidade assimétrica (ALUA) fornece caminhos redundantes e seleção automática de caminhos como parte de qualquer solução de SAN ONTAP. Portanto, não há interrupção de e/S quando o LIF é colocado off-line para o movimento. O host simplesmente tenta novamente e depois move I/o para outro LIF.

Ao usar o movimento LIF, você pode fazer o seguinte sem interrupções:

- Substitua um par de HA de um cluster por um par de HA atualizado de uma forma transparente para os hosts que acessam dados LUN
- Atualize uma placa de interface de destino
- Mova os recursos de uma máquina virtual de storage (SVM) de um conjunto de nós em um cluster para outro conjunto de nós no cluster

Remova um SAN LIF de um conjunto de portas

Se o LIF que você deseja excluir ou mover estiver em um conjunto de portas, você deve remover o LIF do conjunto de portas antes de excluir ou mover o LIF.

Sobre esta tarefa

Você precisa executar o passo 1 no procedimento a seguir somente se um LIF estiver no conjunto de portas. Não é possível remover o último LIF em um conjunto de portas se o conjunto de portas estiver vinculado a um grupo de iniciadores. Caso contrário, você pode começar com a Etapa 2 se várias LIFs estiverem no conjunto de portas.

Passos

1. Se apenas um LIF estiver no conjunto de portas, use o `lun igroup unbind` comando para desvincular o conjunto de portas do grupo de iniciadores.

   > Quando você desvincula um grupo de iniciadores de um conjunto de portas, todos os iniciadores do grupo de iniciadores têm acesso a todos os LUNs de destino mapeados para o grupo de iniciadores em todas as interfaces de rede.

   ```
   cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
   ```

2. Use o `lun portset remove` comando para remover o LIF do conjunto de portas.

   ```
   cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
   ```

Mova um SAN LIF

Se um nó precisar ficar offline, você pode mover um SAN LIF para preservar suas informações de configuração, como o WWPN, e evitar o zoneamento da malha do switch. Como um LIF SAN deve ser colocado off-line antes de ser movido, o tráfego de host deve confiar no software de multipathing de host para fornecer acesso sem interrupções ao LUN. É possível mover SAN LIFs para qualquer nó em um cluster, mas não é possível mover os SAN LIFs entre máquinas virtuais de armazenamento (SVMs).

O que você vai precisar

Se o LIF for um membro de um conjunto de portas, o LIF deve ter sido removido do conjunto de portas antes que o LIF possa ser movido para um nó diferente.

Sobre esta tarefa

O nó de destino e a porta física de um LIF que você deseja mover devem estar na mesma malha FC ou rede Ethernet. Se você mover um LIF para uma malha diferente que não tenha sido corretamente zoneada ou se você mover um LIF para uma rede Ethernet que não tenha conetividade entre o iniciador iSCSI e o destino, o LUN ficará inacessível quando você o colocar novamente on-line.

Passos

1. Veja o status administrativo e operacional do LIF:

   ```
   network interface show -vserver vserver_name
   ```

2. Altere o status do LIF para `down` (offline):

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin
down
```

3. Atribua ao LIF um novo nó e porta:

```
network interface modify -vserver vserver_name -lif LIF_name -home-node
node_name -home-port port_name
```

4. Altere o status do LIF para `up` (online):

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin up
```

5. Verifique as alterações:

```
network interface show -vserver vserver_name
```

Exclua um LIF em um ambiente SAN

Antes de excluir um LIF, você deve garantir que o host conetado ao LIF possa acessar as LUNs por outro caminho.

O que você vai precisar

Se o LIF que você deseja excluir for membro de um conjunto de portas, primeiro remova o LIF do conjunto de portas antes de excluir o LIF.

System Manager

Exclua um LIF com o Gerenciador do sistema ONTAP (9,7 e posterior).

Passos

1. No System Manager, clique em **rede > Visão geral** e selecione **interfaces de rede**.
2. Selecione a VM de armazenamento a partir da qual você deseja excluir o LIF.
3. Clique ⋮ e selecione **Excluir**.

CLI

Exclua um LIF com a CLI do ONTAP.

Passos

1. Verifique o nome do LIF e da porta atual a serem excluídos:

   ```
   network interface show –vserver vserver_name
   ```

2. Eliminar o LIF:

   ```
   network interface delete

   network interface delete -vserver vs1 -lif lif1
   ```

3. Verifique se você excluiu o LIF:

   ```
   network interface show

   network interface show -vserver vs1
   ```

   ```
   Logical Status     Network                    Current   Current Is
   Vserver Interface  Admin/Oper Address/Mask     Node      Port
   Home
   ------- ---------- ---------- ---------------- --------- -------
   ----
   vs1
           lif2       up/up      192.168.2.72/24  node-01   e0b
   true
           lif3       up/up      192.168.2.73/24  node-01   e0b
   true
   ```

Requisitos de SAN LIF para adicionar nós a um cluster

Você precisa estar ciente de certas considerações ao adicionar nós a um cluster.

- É necessário criar LIFs nos novos nós conforme apropriado antes de criar LUNs nesses novos nós.
- É necessário descobrir esses LIFs dos hosts conforme ditado pela pilha e pelo protocolo de host.

- Você deve criar LIFs nos novos nós para que os movimentos de LUN e volume sejam possíveis sem usar a rede de interconexão de cluster.

Configure iSCSI LIFs para retornar FQDN para hospedar a operação iSCSI SendTargets Discovery

A partir do ONTAP 9, os LIFs iSCSI podem ser configurados para retornar um nome de domínio totalmente qualificado (FQDN) quando um sistema operacional host envia uma operação de descoberta de SendTargets iSCSI. Retornar um FQDN é útil quando há um dispositivo NAT (Network Address Translation) entre o sistema operacional do host e o serviço de armazenamento.

Sobre esta tarefa

Os endereços IP de um lado do dispositivo NAT não têm sentido no outro lado, mas os FQDNs podem ter significado em ambos os lados.

> O limite de interoperabilidade do valor FQDN é de 128 carateres em todos os sistemas operacionais host.

Passos

1. Altere a configuração de privilégios para avançado:

   ```
   set -privilege advanced
   ```

2. Configurar iSCSI LIFs para retornar FQDN:

   ```
   vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name
   -sendtargets_fqdn FQDN
   ```

   No exemplo a seguir, os LIFs iSCSI são configurados para retornar storagehost-005.example.com como FQDN.

   ```
   vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn
   storagehost-005.example.com
   ```

3. Verifique se sendtargets é o FQDN:

   ```
   vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
   ```

   Neste exemplo, storagehost-005.example.com é exibido no campo de saída sendtargets-fqdn.

   ```
   cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields
   sendtargets-fqdn
   vserver lif        sendtargets-fqdn
   ------- ---------- --------------------------
   vs1     vs1_iscsi1 storagehost-005.example.com
   vs1     vs1_iscsi2 storagehost-006.example.com
   ```

Informações relacionadas

"Referência do comando ONTAP"

Ativar a alocação de espaço ONTAP para protocolos SAN

A alocação de espaço do ONTAP ajuda a impedir que seus LUNs ou namespaces NVMe fiquem offline se eles ficarem sem espaço e permitir que seus hosts SAN recuperem espaço.

O suporte da ONTAP para alocação de espaço é baseado no protocolo SAN e na versão do ONTAP. A partir do ONTAP 9.16,1, a alocação de espaço é habilitada por padrão para protocolos iSCSI, FC e NVMe para todos os LUNs e namespaces recém-criados.

Versão de ONTAP	Protocolos	A alocação de espaço é…
9.16.1 ou posterior	• ISCSI • FC • NVMe	Habilitado por padrão para LUNs e namespaces recém-criados
9.15.1	• ISCSI • FC	Habilitado por padrão para LUNs recém-criados
	NVMe	Não suportado
9.14.1 e anteriores	• ISCSI • FC	Desativado por padrão para LUNs recém-criados
	NVMe	Não suportado

Quando a alocação de espaço está ativada:

- Se um LUN ou namespace ficar sem espaço, o ONTAP se comunica com o host que nenhum espaço livre está disponível para operações de gravação. Como resultado, o LUN ou namespace permanece on-line e as operações de leitura continuam sendo atendidas. Dependendo da configuração do host, o host tenta novamente as operações de gravação até que ele seja bem-sucedido ou o sistema de arquivos do host seja colocado offline. As operações de gravação são retomadas quando espaço livre adicional se torna disponível para o LUN ou namespace.

  Se a alocação de espaço não estiver ativada, quando um LUN ou namespace ficar sem espaço, todas as operações de e/S falharão e o LUN ou namespace for colocado off-line; o problema de espaço deve ser resolvido para retomar as operações normais. A nova digitalização de dispositivos LUN também pode ser necessária no host para restaurar caminhos e dispositivos para um estado operacional.

- Um host pode executar operações SCSI ou NVMe `UNMAP` (às vezes chamadas `TRIM`). As operações DE DESMAPEAMENTO permitem que um host identifique blocos de dados que não são mais necessários porque eles não contêm mais dados válidos. A identificação normalmente acontece após a exclusão do arquivo. O sistema de armazenamento pode então desalocar esses blocos de dados para que o espaço possa ser consumido em outro lugar. Essa realocação melhora significativamente a eficiência geral de armazenamento, especialmente com sistemas de arquivos que têm alta rotatividade de dados.

Antes de começar

A ativação da alocação de espaço requer uma configuração de host que possa lidar corretamente com erros de alocação de espaço quando uma gravação não pode ser concluída. A utilização de SCSI ou NVMe `UNMAP` requer uma configuração que possa usar o provisionamento de bloco lógico conforme definido no padrão

SCSI SBC-3.

Os hosts a seguir atualmente oferecem suporte a thin Provisioning quando você ativa a alocação de espaço:

- Citrix XenServer 6,5 e posterior
- VMware ESXi 5,0 e posterior
- Kernel Oracle Linux 6,2 UEK e posterior
- Red Hat Enterprise Linux 6,2 e posterior
- SUSE Linux Enterprise Server 11 e posterior
- Solaris 11,1 e posterior
- Windows

Sobre esta tarefa

Quando você atualiza seu cluster para o ONTAP 9.15,1 ou posterior, a configuração de alocação de espaço para todos os LUNs criados antes da atualização de software permanece a mesma após a atualização, independentemente do tipo de host. Por exemplo, se um LUN foi criado no ONTAP 9.13,1 para um host VMware com alocação de espaço desativada, a alocação de espaço nesse LUN permanecerá desativada após a atualização para o ONTAP 9.15,1.

Passos

1. Ativar alocação de espaço:

```
lun modify -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-space-allocation enabled
```

2. Verifique se a alocação de espaço está ativada:

```
lun show -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-fields space-allocation
```

3. Verifique se a alocação de espaço está ativada no sistema operacional do host.

> Algumas configurações de host, incluindo algumas versões do VMware ESXi, podem reconhecer automaticamente a alteração de configuração e não exigem intervenção do usuário. Outras configurações podem exigir uma nova digitalização do dispositivo. Alguns sistemas de arquivos e gerenciadores de volume podem exigir configurações específicas adicionais para habilitar a recuperação de espaço usando `SCSI UNMAP`o . A reinstalação de sistemas de arquivos ou uma reinicialização total do sistema operacional pode ser necessária. Consulte a documentação do seu host específico para obter orientação.

Configuração de host para hosts NVMe posteriores e VMware ESXi 8.x

Se você tiver um host VMware executando o ESXi 8.x ou posterior com o protocolo NVMe, depois de ativar a alocação de espaço no ONTAP, execute as etapas a seguir nos hosts.

Passos

1. No seu anfitrião ESXi, verifique se o DSM está desativado:

   ```
   esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
   ```

   O valor esperado é 0.

2. Ativar o NVMe DSM:

   ```
   esxcfg-advcfg -s 1 /Scsi/NvmeUseDsmTp4040
   ```

3. Verifique se o DSM está ativado:

   ```
   esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
   ```

   O valor esperado é 1.

Links relacionados

Saiba mais "Configuração de host NVMe-of para ESXi 8.x com ONTAP"sobre o .

Combinações recomendadas de volume e arquivo ou configuração LUN

Visão geral das combinações recomendadas de volume e arquivo ou configuração LUN

Existem combinações específicas de configurações de FlexVol volume e arquivo ou LUN que você pode usar, dependendo dos requisitos de aplicação e administração. Compreender os benefícios e os custos dessas combinações pode ajudá-lo a determinar a combinação certa de configuração de volume e LUN para o seu ambiente.

As seguintes combinações de configuração de volume e LUN são recomendadas:

- Arquivos ou LUNs com espaço reservado com provisionamento de volume espesso
- LUNs ou arquivos não reservados ao espaço com provisionamento de thin volumes
- Arquivos ou LUNs com espaço reservado com provisionamento de volume semi-espesso

Você pode usar o thin Provisioning SCSI em seus LUNs em conjunto com qualquer uma dessas combinações de configuração.

Arquivos ou LUNs com espaço reservado com provisionamento de volume espesso

Benefícios:

- Todas as operações de gravação dentro de arquivos reservados ao espaço são garantidas; elas não falharão devido a espaço insuficiente.
- Não há restrições quanto à eficiência de storage e às tecnologias de proteção de dados no volume.

Custos e limitações:

- Espaço suficiente deve ser separado do agregado na frente para suportar o volume provisionado thickly.
- O espaço igual a duas vezes o tamanho do LUN é alocado do volume no momento da criação do LUN.

LUNs ou arquivos não reservados ao espaço com provisionamento de thin volumes

Benefícios:

- Não há restrições quanto à eficiência de storage e às tecnologias de proteção de dados no volume.
- O espaço é alocado apenas como é usado.

Custos e restrições:

- As operações de gravação não são garantidas; elas podem falhar se o volume ficar sem espaço livre.
- Você deve gerenciar o espaço livre no agregado de forma eficaz para evitar que o agregado fique sem espaço livre.

Arquivos ou LUNs com espaço reservado com provisionamento de volume semi-espesso

Benefícios:

Há menos espaço reservado antes do que para o provisionamento de volume espesso, e ainda é fornecida uma garantia de gravação melhor esforço.

Custos e restrições:

- Operações de gravação podem falhar com essa opção.

  Você pode mitigar esse risco equilibrando adequadamente o espaço livre no volume em relação à volatilidade dos dados.

- Não é possível confiar na retenção de objetos de proteção de dados, como cópias Snapshot, arquivos FlexClone e LUNs.
- Você não pode usar os recursos de eficiência de storage de compartilhamento de bloco do ONTAP que não podem ser excluídos automaticamente, incluindo deduplicação, compactação e descarregamento de cópias/ODX.

Determine a combinação correta de volume e configuração LUN para o seu ambiente

Responder a algumas perguntas básicas sobre o seu ambiente pode ajudá-lo a determinar a melhor configuração de FlexVol volume e LUN para o seu ambiente.

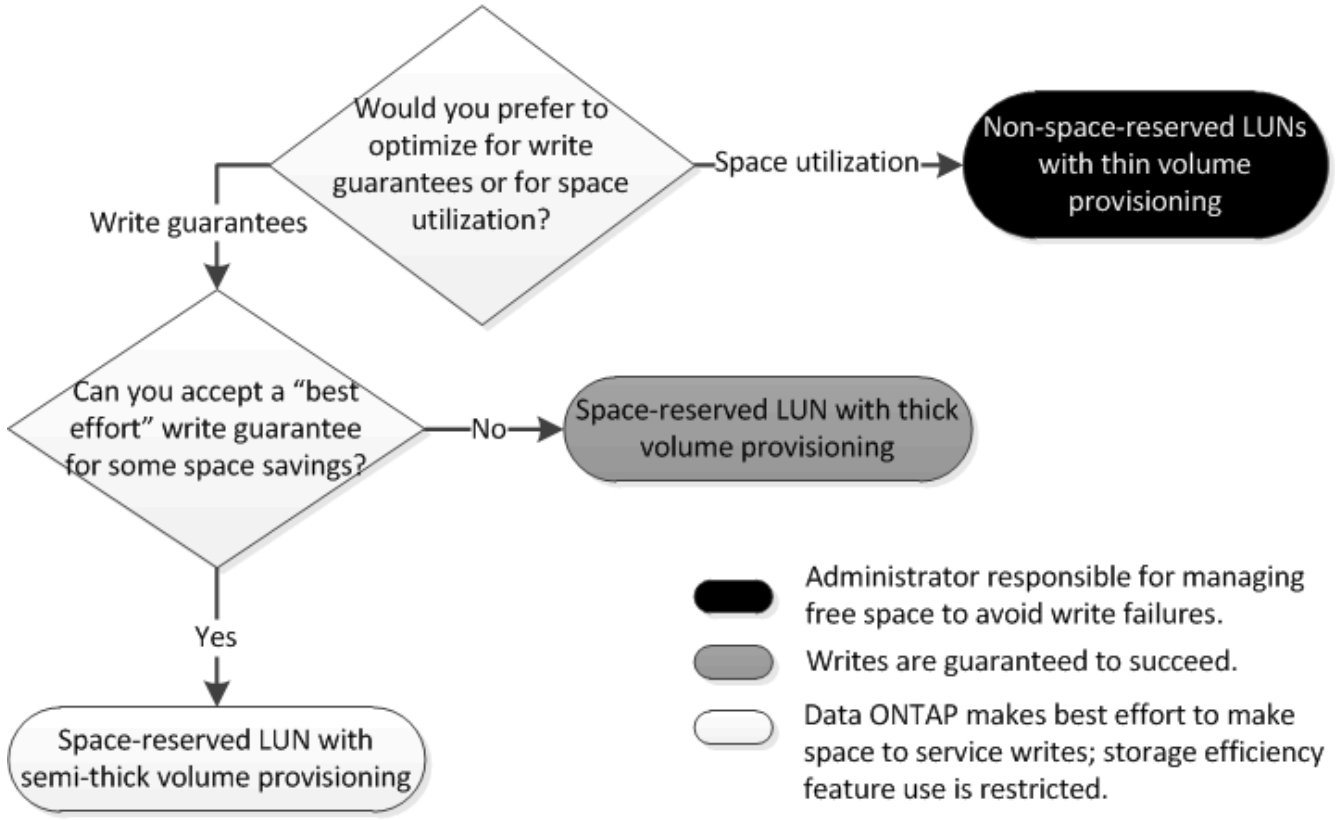
Sobre esta tarefa

Você pode otimizar as configurações de LUN e volume para a máxima utilização do storage ou para a segurança das garantias de gravação. Com base nos requisitos de utilização do storage e na capacidade de monitorar e reabastecer o espaço livre rapidamente, é necessário determinar os volumes de FlexVol volume e LUN apropriados para sua instalação.

Não é necessário um volume separado para cada LUN.

Passo

1. Use a seguinte árvore de decisão para determinar a melhor combinação de volume e configuração LUN para o seu ambiente:



Calcule a taxa de crescimento de dados para LUNs

Você precisa saber a taxa com que seus dados LUN estão crescendo ao longo do tempo para determinar se você deve usar LUNs com espaço reservado ou LUNs não reservados.

Sobre esta tarefa

Se você tiver uma taxa consistente de crescimento de dados, as LUNs com espaço reservado podem ser a melhor opção para você. Se você tiver uma taxa baixa de crescimento de dados, considere LUNs não reservados para espaço.

Você pode usar ferramentas como o OnCommand Insight para calcular a taxa de crescimento de dados ou calculá-la manualmente. As etapas a seguir são para cálculo manual.

Passos

1. Configure um LUN com espaço reservado.
2. Monitorize os dados no LUN durante um período de tempo definido, como uma semana.

   Certifique-se de que seu período de monitoramento é longo o suficiente para formar uma amostra representativa de aumentos regulares no crescimento de dados. Por exemplo, é possível que você tenha uma grande quantidade de crescimento de dados consistentemente no final de cada mês.

3. Todos os dias, Registre em GB quanto seus dados crescem.
4. No final do período de monitoramento, adicione os totais de cada dia juntos e divida pelo número de dias no período de monitoramento.

   Este cálculo produz a sua taxa média de crescimento.

Exemplo

Neste exemplo, você precisa de um LUN de 200 GB. Você decide monitorar o LUN por uma semana e Registrar as seguintes alterações diárias de dados:

- Domingo: 20 GB
- Segunda-feira: 18 GB
- Terça-feira: 17 GB
- Quarta-feira: 20 GB
- Quinta-feira: 20 GB
- Sexta-feira: 23 GB
- Sábado: 22 GB

Neste exemplo, sua taxa de crescimento é (20-18-17-20-20-23-22) / 7 é de 20 GB por dia.

Definições de configuração para ficheiros reservados ao espaço ou LUNs com volumes provisionados de espessura

Essa combinação de configuração de FlexVol volume e arquivo ou LUN permite usar tecnologias de eficiência de storage e não exige que você monitore ativamente o espaço livre, pois há espaço suficiente alocado inicialmente.

As configurações a seguir são necessárias para configurar um arquivo ou LUN com espaço reservado em um volume usando provisionamento espesso:

Definição do volume	Valor
Garantia	Volume
Reserva fracionária	100
Reserva do Snapshot	Qualquer
snapshot Autodelete	Opcional
Crescimento automático	Opcional; se ativado, o espaço livre agregado deve ser monitorado ativamente.

Configuração de arquivo ou LUN	Valor
Reserva de espaço	Ativado

Configurações para arquivos não reservados ao espaço ou LUNs com volumes provisionados com thin

Essa combinação de configuração de FlexVol volume e arquivo ou LUN exige que a menor quantidade de storage seja alocada antes, mas requer gerenciamento ativo de espaço livre para evitar erros devido à falta de espaço.

As seguintes configurações são necessárias para configurar um LUN ou arquivos não reservados ao espaço em um volume provisionado com thin:

Definição do volume	Valor
Garantia	Nenhum
Reserva fracionária	0
Reserva do Snapshot	Qualquer
snapshot Autodelete	Opcional
Crescimento automático	Opcional

Configuração de arquivo ou LUN	Valor
Reserva de espaço	Desativado

Considerações adicionais

Quando o volume ou agregado ficar sem espaço, as operações de gravação no arquivo ou LUN podem falhar.

Se você não quiser monitorar ativamente o espaço livre tanto para o volume quanto para o agregado, ative o crescimento automático para o volume e defina o tamanho máximo para o volume como o tamanho do agregado. Nessa configuração, você deve monitorar ativamente o espaço livre agregado, mas não precisa monitorar o espaço livre no volume.

Configurações para arquivos reservados ao espaço ou LUNs com provisionamento de volume semi-espesso

Essa combinação de configuração de FlexVol volume e arquivo ou LUN requer menos storage para ser alocado antes do que a combinação totalmente provisionada, mas impõe restrições às tecnologias de eficiência que você pode usar para o volume. As substituições são cumpridas com o melhor esforço para essa combinação de configuração.

As configurações a seguir são necessárias para configurar um LUN com espaço reservado em um volume usando provisionamento semi-espesso:

Definição do volume	Valor
Garantia	Volume
Reserva fracionária	0
Reserva do Snapshot	0

Definição do volume	Valor
snapshot Autodelete	On, com um nível de compromisso de destruir, uma lista de destruir que inclui todos os objetos, o gatilho definido para volume e todos os LUNs e arquivos FlexClone FlexClone ativados para exclusão automática.
Crescimento automático	Opcional; se ativado, o espaço livre agregado deve ser monitorado ativamente.

Configuração de arquivo ou LUN	Valor
Reserva de espaço	Ativado

Restrições tecnológicas

Você não pode usar as seguintes tecnologias de eficiência de storage de volume para essa combinação de configuração:

- Compactação
- Deduplicação
- Descarregar cópias ODX e FlexClone
- LUNs e arquivos FlexClone do FlexClone não marcados para exclusão automática (clones ativos)
- Subficheiros FlexClone
- Descarregar ODX/Copy

Considerações adicionais

Os seguintes fatos devem ser considerados ao empregar esta combinação de configuração:

- Quando o volume compatível com o LUN é executado com pouco espaço, os dados de proteção (LUNs e arquivos FlexClone, cópias Snapshot) são destruídos.
- As operações de gravação podem ter tempo limite e falhar quando o volume ficar sem espaço livre.

A compactação é ativada por padrão para plataformas AFF. Você deve desativar explicitamente a compactação para qualquer volume para o qual deseja usar o provisionamento semi-espesso em uma plataforma AFF.

Proteção de dados SAN

Visão geral dos métodos de proteção de dados em ambientes SAN

Você pode proteger seus dados fazendo cópias deles para que fiquem disponíveis para restauração em caso de exclusão acidental, falhas no aplicativo, corrupção de dados ou desastre. Dependendo das suas necessidades de proteção e backup de dados, o ONTAP oferece uma variedade de métodos que permitem proteger seus dados.

Sincronização ativa do SnapMirror

A partir da disponibilidade geral no ONTAP 9.9,1, fornece objetivo de tempo de recuperação zero (rto zero) ou failover transparente de aplicações (TAF) para permitir o failover automático de aplicações essenciais aos negócios em ambientes SAN. O SnapMirror active Sync requer a instalação do ONTAP Mediator 1,2 em uma configuração com dois clusters AFF ou dois clusters All-Flash SAN Array (ASA).

"Sincronização ativa do SnapMirror"

Cópia Snapshot

Permite criar, agendar e manter, manualmente ou automaticamente, vários backups dos LUNs. As cópias snapshot usam apenas uma quantidade mínima de espaço de volume adicional e não têm custo de performance. Se seus dados LUN forem modificados ou excluídos acidentalmente, esses dados poderão ser restaurados de forma fácil e rápida a partir de uma das cópias Snapshot mais recentes.

FlexClone LUNs (é necessária licença FlexClone)

Fornece cópias graváveis e pontuais de outro LUN em um volume ativo ou em uma cópia Snapshot. Um clone e seu pai podem ser modificados independentemente sem afetar um ao outro.

SnapRestore (licença necessária)

Permite realizar uma recuperação de dados rápida, com uso eficiente de espaço e sob solicitação de cópias Snapshot em um volume inteiro. Você pode usar o SnapRestore para restaurar um LUN para um estado preservado anterior sem reiniciar o sistema de armazenamento.

Cópias espelhadas de proteção de dados (é necessária licença SnapMirror)

Fornece recuperação assíncrona de desastres, permitindo que você crie periodicamente cópias Snapshot de dados em seu volume, copie essas cópias Snapshot em uma rede local ou de área ampla para um volume de parceiro, geralmente em outro cluster e retenha essas cópias Snapshot. A cópia espelhada no volume do parceiro fornece disponibilidade e restauração rápidas dos dados a partir do momento da última cópia Snapshot, se os dados no volume de origem estiverem corrompidos ou perdidos.

Backups do SnapVault (é necessária licença SnapMirror)

Fornece retenção eficiente de backups a longo prazo e storage. Os relacionamentos do SnapVault permitem que você faça backup de cópias Snapshot selecionadas de volumes para um volume de destino e retenha os backups.

Se você conduzir backups em fita e operações de arquivamento, poderá executá-los nos dados que já tiverem backup no volume secundário do SnapVault.

SnapDrive para Windows ou UNIX (é necessária licença SnapDrive)

Configura o acesso a LUNs, gerencia LUNs e gerencia cópias Snapshot do sistema de storage diretamente de hosts Windows ou UNIX.

Backup e recuperação em fita nativa

O suporte para a maioria das unidades de fita existentes está incluído no ONTAP, bem como um método para que os fornecedores de fita adicionem suporte dinâmico a novos dispositivos. O ONTAP também suporta o protocolo de fita magnética remota (RMT), permitindo backup e recuperação para qualquer sistema capaz.

Informações relacionadas

"Documentação do NetApp: SnapDrive para UNIX"

"Documentação do NetApp: SnapDrive para Windows (versões atuais)"

"Proteção de dados usando backup em fita"

Efeito da movimentação ou cópia de um LUN em cópias Snapshot

Efeito da movimentação ou cópia de um LUN na visão geral das cópias Snapshot

As cópias snapshot são criadas no nível do volume. Se você copiar ou mover um LUN para um volume diferente, a política de cópia Snapshot da voluna de destino será aplicada ao volume copiado ou movido. Se as cópias Snapshot não estiverem estabelecidas para o volume de destino, as cópias Snapshot não serão criadas do LUN movido ou copiado.

Restaure um único LUN a partir de uma cópia Snapshot

Você pode restaurar um único LUN de uma cópia Snapshot sem restaurar todo o volume que contém o único LUN. Você pode restaurar o LUN no lugar ou para um novo caminho no volume. A operação restaura apenas o único LUN sem afetar outros arquivos ou LUNs no volume. Você também pode restaurar arquivos com streams.

O que você vai precisar

- Você deve ter espaço suficiente no volume para concluir a operação de restauração:
  - Se você estiver restaurando um LUN com espaço reservado em que a reserva fracionária seja de 0%, será necessário uma vez o tamanho do LUN restaurado.
  - Se você estiver restaurando um LUN com espaço reservado em que a reserva fracionária seja de 100%, será necessário duas vezes o tamanho do LUN restaurado.
  - Se você estiver restaurando um LUN não reservado com espaço, você só precisará do espaço real usado para o LUN restaurado.
- Uma cópia Snapshot do LUN de destino deve ter sido criada.

  Se a operação de restauração falhar, o LUN de destino pode ser truncado. Nesses casos, você pode usar a cópia Snapshot para evitar a perda de dados.

- Uma cópia Snapshot do LUN de origem deve ter sido criada.

  Em casos raros, a restauração LUN pode falhar, deixando o LUN de origem inutilizável. Se isso ocorrer, você pode usar a cópia Snapshot para retornar o LUN ao estado imediatamente antes da tentativa de restauração.

- O LUN de destino e o LUN de origem têm de ter o mesmo tipo de SO.

  Se o LUN de destino tiver um tipo de SO diferente do LUN de origem, o anfitrião poderá perder o acesso aos dados ao LUN de destino após a operação de restauro.

Passos

1. A partir do host, pare todo o acesso do host ao LUN.
2. Desmonte o LUN em seu host para que o host não possa acessar o LUN.
3. Desmapear o LUN:

   `lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name -igroup igroup_name`

4. Determine a cópia Snapshot para a qual deseja restaurar o LUN:

   `volume snapshot show -vserver vserver_name -volume volume_name`

5. Crie uma cópia Snapshot do LUN antes de restaurar o LUN:

   `volume snapshot create -vserver vserver_name -volume volume_name -snapshot snapshot_name`

6. Restaure o LUN especificado em um volume:

   `volume snapshot restore-file -vserver vserver_name -volume volume_name -snapshot snapshot_name -path lun_path`

7. Siga os passos apresentados no ecrã.
8. Se necessário, coloque o LUN online:

   `lun modify -vserver vserver_name -path lun_path -state online`

9. Se necessário, remapear o LUN:

   `lun mapping create -vserver vserver_name -volume volume_name -lun lun_name -igroup igroup_name`

10. Do host, remonte o LUN.
11. A partir do host, reinicie o acesso ao LUN.

Restaurar todos os LUNs em um volume a partir de uma cópia Snapshot

Você pode usar `volume snapshot restore` o comando para restaurar todos os LUNs em um volume especificado a partir de uma cópia Snapshot.

Passos

1. No host, interrompa todo o acesso do host aos LUNs.

   Usar o SnapRestore sem interromper todo o acesso do host aos LUNs no volume pode causar corrupção de dados e erros do sistema.

2. Desmonte os LUNs nesse host para que o host não possa acessar os LUNs.
3. Desmapear os LUNs:

   `lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name -igroup igroup_name`

4. Determine a cópia Snapshot para a qual você deseja restaurar o volume:

   `volume snapshot show -vserver vserver_name -volume volume_name`

5. Altere a configuração de privilégio para avançado:

   `set -privilege advanced`

6. Restaure seus dados:

   `volume snapshot restore -vserver vserver_name -volume volume_name -snapshot snapshot_name`

7. Siga as instruções apresentadas no ecrã.
8. Remapear os LUNs:

   `lun mapping create -vserver vserver_name -volume volume_name -lun lun_name -igroup igroup_name`

9. Verifique se os LUNs estão online:

   `lun show -vserver vserver_name -path lun_path -fields state`

10. Se os LUNs não estiverem online, coloque-os online:

    `lun modify -vserver vserver_name -path lun_path -state online`

11. Altere a configuração de privilégios para admin:

    `set -privilege admin`

12. No host, remonte seus LUNs.
13. No host, reinicie o acesso aos LUNs.

Exclua uma ou mais cópias Snapshot existentes de um volume

Você pode excluir manualmente uma ou mais cópias Snapshot existentes do volume. Você pode querer fazer isso se precisar de mais espaço em seu volume.

Passos

1. Use o `volume snapshot show` comando para verificar quais cópias snapshot você deseja excluir.

```
cluster::> volume snapshot show -vserver vs3 -volume vol3

                                                  ---Blocks---
Vserver  Volume  Snapshot                  Size   Total% Used%
-------- ------- ------------------------ -----  ------ -----
vs3      vol3
                 snap1.2013-05-01_0015   100KB   0%    38%
                 snap1.2013-05-08_0015   76KB    0%    32%
                 snap2.2013-05-09_0010   76KB    0%    32%
                 snap2.2013-05-10_0010   76KB    0%    32%
                 snap3.2013-05-10_1005   72KB    0%    31%
                 snap3.2013-05-10_1105   72KB    0%    31%
                 snap3.2013-05-10_1205   72KB    0%    31%
                 snap3.2013-05-10_1305   72KB    0%    31%
                 snap3.2013-05-10_1405   72KB    0%    31%
                 snap3.2013-05-10_1505   72KB    0%    31%
10 entries were displayed.
```

2. Use o `volume snapshot delete` comando para excluir cópias Snapshot.

Se você quiser…	Digite este comando…
Excluir uma única cópia Snapshot	`volume snapshot delete -vserver` *`svm_name`* `-volume` *`vol_name`* `-snapshot` *`snapshot_name`*
Exclua várias cópias Snapshot	`volume snapshot delete -vserver` *`svm_name`* `-volume` *`vol_name`* `-snapshot` *`snapshot_name1`*`[,`*`snapshot_name2`*`,…]`
Excluir todas as cópias Snapshot	`volume snapshot delete -vserver` *`svm_name`* `-volume` *`vol_name`* `-snapshot *`

O exemplo a seguir exclui todas as cópias Snapshot no volume vol3.

```
cluster::> volume snapshot delete -vserver vs3 -volume vol3 *

10 entries were acted on.
```

Use LUNs do FlexClone para proteger seus dados

Use LUNs FlexClone para proteger a visão geral dos dados

Um LUN FlexClone é uma cópia gravável e pontual de outro LUN em um volume ativo ou

em uma cópia Snapshot. O clone e seu pai podem ser modificados independentemente sem afetar um ao outro.

Um LUN FlexClone compartilha espaço inicialmente com seu LUN pai. Por padrão, o LUN FlexClone herda o atributo espaço reservado do LUN pai. Por exemplo, se o LUN pai não for reservado com espaço, o LUN FlexClone também não é reservado com espaço por padrão. No entanto, você pode criar um LUN FlexClone não reservado com espaço a partir de um pai que seja um LUN reservado com espaço.

Quando você clonar um LUN, o compartilhamento de bloco ocorre em segundo plano e não é possível criar uma cópia Snapshot de volume até que o compartilhamento de bloco seja concluído.

Tem de configurar o volume para ativar a função de eliminação automática LUN FlexClone com o `volume snapshot autodelete modify` comando. Caso contrário, se você quiser que os LUNs do FlexClone sejam excluídos automaticamente, mas o volume não estiver configurado para a exclusão automática do FlexClone, nenhum dos LUNs do FlexClone será excluído.

Quando você cria um LUN FlexClone, a função de exclusão automática FlexClone LUN é desativada por padrão. Você deve ativá-lo manualmente em cada LUN FlexClone antes que esse LUN FlexClone possa ser excluído automaticamente. Se você estiver usando o provisionamento de volume semi-espesso e quiser a garantia de gravação "melhor esforço" fornecida por essa opção, você deve disponibilizar *All* FlexClone LUNs para exclusão automática.

> Quando você cria um LUN FlexClone a partir de uma cópia Snapshot, o LUN é automaticamente dividido da cópia Snapshot usando um processo em segundo plano com uso eficiente de espaço para que o LUN não continue a depender da cópia Snapshot ou consumir nenhum espaço adicional. Se esta divisão em segundo plano não tiver sido concluída e esta cópia Snapshot for automaticamente eliminada, esse LUN FlexClone será eliminado mesmo que tenha desativado a função de eliminação automática do FlexClone para esse LUN FlexClone. Depois que a divisão em segundo plano estiver concluída, o LUN FlexClone não será excluído mesmo que essa cópia Snapshot seja excluída.

Informações relacionadas

"Gerenciamento de storage lógico"

Razões para usar LUNs FlexClone

Você pode usar LUNs do FlexClone para criar várias cópias de leitura/gravação de um LUN.

Você pode querer fazer isso pelas seguintes razões:

- Você precisa criar uma cópia temporária de um LUN para fins de teste.
- Você precisa disponibilizar uma cópia de seus dados para usuários adicionais sem dar acesso aos dados de produção.
- Você deseja criar um clone de um banco de dados para operações de manipulação e projeção, preservando os dados originais de uma forma inalterada.
- Você deseja acessar um subconjunto específico de dados de um LUN (um volume lógico específico ou sistema de arquivos em um grupo de volumes ou um arquivo específico ou conjunto de arquivos em um sistema de arquivos) e copiá-lo para o LUN original, sem restaurar o restante dos dados no LUN original. Isso funciona em sistemas operacionais que suportam a montagem de um LUN e um clone do LUN ao mesmo tempo. O SnapDrive para UNIX suporta isso com o `snap connect` comando.

- Você precisa de vários hosts de inicialização SAN com o mesmo sistema operacional.

Como um FlexVol volume pode recuperar espaço livre com a configuração de transferência de dados

Pode ativar a definição de FlexVol volume para eliminar automaticamente ficheiros FlexClone e LUNs FlexClone. Ao ativar o serviço de correio eletrónico, pode recuperar uma quantidade alvo de espaço livre no volume quando um volume estiver quase cheio.

Você pode configurar um volume para começar a excluir automaticamente arquivos FlexClone e LUNs FlexClone quando o espaço livre no volume diminuir abaixo de um determinado valor limite e parar automaticamente de excluir clones quando uma quantidade de espaço livre no volume for recuperada. Embora não seja possível especificar o valor de limite que inicia a exclusão automática de clones, você pode especificar se um clone é elegível para exclusão e especificar a quantidade de espaço livre de destino para um volume.

Um volume exclui automaticamente arquivos FlexClone e LUNs FlexClone quando o espaço livre no volume diminui abaixo de um determinado limite e quando *ambos* dos seguintes requisitos são atendidos:

- A funcionalidade de autodelete está ativada para o volume que contém os arquivos FlexClone e LUNs FlexClone.

  Você pode ativar a capacidade de transferência de um FlexVol volume usando o `volume snapshot autodelete modify` comando. Você deve definir o `-trigger` parâmetro para `volume` ou `snap_reserve` para que um volume exclua automaticamente arquivos FlexClone e LUNs FlexClone.

- A funcionalidade de configuração do sistema de áudio e vídeo é habilitada para os LUNs FlexClone e FlexClone.

  Você pode ativar o arquivo FlexClone ou FlexClone LUN usando o `file clone create` comando com o `-autodelete` parâmetro. Como resultado, você pode preservar certos arquivos FlexClone e LUNs FlexClone, desativando o serviço de seleção de clones e garantindo que outras configurações de volume não substituam a configuração de clone.

Configure um FlexVol volume para excluir automaticamente arquivos FlexClone e LUNs FlexClone

Pode ativar um FlexVol volume para eliminar automaticamente ficheiros FlexClone e LUNs FlexClone com o sistema de gestão de dados em curso ativado quando o espaço livre no volume diminui abaixo de um determinado limite.

O que você vai precisar

- O FlexVol volume deve conter arquivos FlexClone e LUNs FlexClone e estar online.
- O FlexVol volume não deve ser um volume somente leitura.

Passos

1. Ative a exclusão automática de arquivos FlexClone e LUNs FlexClone no FlexVol volume usando o `volume snapshot autodelete modify` comando.
   - Para o `-trigger` parâmetro, pode especificar `volume` ou `snap_reserve`.
   - Para o `-destroy-list` parâmetro, você deve sempre especificar `lun_clone,file_clone`, independentemente de você querer excluir apenas um tipo de clone. O exemplo a seguir mostra como você pode ativar o volume vol1 para acionar a exclusão automática de arquivos FlexClone e LUNs

FlexClone para recuperação de espaço até que 25% do volume consista em espaço livre:

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume
vol1 -enabled true -commitment disrupt -trigger volume -target-free
-space 25 -destroy-list lun_clone,file_clone

Volume modify successful on volume:vol1
```

> Ao ativar volumes FlexVol para exclusão automática, se você definir o valor `-commitment` do parâmetro como `destroy`, todos os arquivos FlexClone e LUNs FlexClone com o `-autodelete` parâmetro definido como `true` poderão ser excluídos quando o espaço livre no volume diminuir abaixo do valor de limite especificado. No entanto, os arquivos FlexClone e LUNs FlexClone com o `-autodelete` parâmetro definido como `false` não serão excluídos.

2. Verifique se a exclusão automática de arquivos FlexClone e LUNs FlexClone está ativada no FlexVol volume usando o `volume snapshot autodelete show` comando.

   O exemplo a seguir mostra que o volume vol1 está habilitado para exclusão automática de arquivos FlexClone e LUNs FlexClone:

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1

         Vserver Name: vs1
          Volume Name: vol1
          Enabled: true
            Commitment: disrupt
         Defer Delete: user_created
         Delete Order: oldest_first
  Defer Delete Prefix: (not specified)*
    Target Free Space: 25%
              Trigger: volume
     Destroy List: lun_clone,file_clone
Is Constituent Volume: false
```

3. Certifique-se de que o serviço de correio eletrónico está ativado para os ficheiros FlexClone e LUNs FlexClone no volume que pretende eliminar, executando as seguintes etapas:

   a. Ative a exclusão automática de um arquivo FlexClone específico ou LUN FlexClone usando o `volume file clone autodelete` comando.

      Você pode forçar um arquivo FlexClone específico ou LUN FlexClone a ser automaticamente excluído usando o `volume file clone autodelete` comando com o `-force` parâmetro.

      O exemplo a seguir mostra que a exclusão automática do FlexClone LUN lun1_clone contido no volume vol1 está ativada:

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path
/vol/vol1/lun1_clone -enabled true
```

Você pode ativar o arquivo FlexClone e LUNs do FlexClone.

b. Verifique se o arquivo FlexClone ou FlexClone LUN está habilitado para exclusão automática usando o `volume file clone show-autodelete` comando.

O exemplo a seguir mostra que o FlexClone LUN lun1_clone está habilitado para exclusão automática:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone
-path vol/vol1/lun1_clone
                                                                Vserver
Name: vs1
                                                                Clone
Path: vol/vol1/lun1_clone

**Autodelete Enabled: true**
```

Para obter mais informações sobre como usar os comandos, consulte as respetivas páginas de manual.

Clonar LUNs de um volume ativo

É possível criar cópias dos LUNs clonando os LUNs no volume ativo. Esses LUNs FlexClone são cópias legíveis e graváveis dos LUNs originais no volume ativo.

> Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga "estes passos" para clonar dados. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

O que você vai precisar

Uma licença FlexClone deve ser instalada. Esta licença está incluída no "ONTAP One".

Sobre esta tarefa

Um LUN FlexClone reservado com espaço requer tanto espaço quanto o LUN pai reservado com espaço. Se o LUN FlexClone não tiver espaço reservado, você deve garantir que o volume tenha espaço suficiente para acomodar alterações no LUN FlexClone.

Passos

1. Você deve ter verificado que os LUNs não são mapeados para um iggroup ou são gravados antes de fazer o clone.
2. Use o `lun show` comando para verificar se o LUN existe.

```
lun show -vserver vs1
```

```
Vserver  Path                State     Mapped    Type      Size
-------- ------------------ --------- --------- -------- -------
vs1      /vol/vol1/lun1     online    unmapped  windows  47.07MB
```

3. Use o `volume file clone create` comando para criar o LUN FlexClone.

   ```
   volume file clone create -vserver vs1 -volume vol1 -source-path lun1
   -destination-path/lun1_clone
   ```

   Se você precisar que o LUN FlexClone esteja disponível para exclusão automática, inclua `-autodelete true`o . Se você estiver criando esse LUN FlexClone em um volume usando provisionamento semi-espesso, será necessário habilitar a exclusão automática para todos os LUNs FlexClone.

4. Use o `lun show` comando para verificar se você criou um LUN.

   ```
   lun show -vserver vs1
   ```

```
Vserver  Path                      State    Mapped   Type      Size
-------- ------------------------ -------- -------- -------- ------
vs1      /vol/volX/lun1           online   unmapped windows  47.07MB
vs1      /vol/volX/lun1_clone     online   unmapped windows  47.07MB
```

Criar LUNs FlexClone a partir de uma cópia Snapshot em um volume

Você pode usar uma cópia Snapshot no volume para criar cópias FlexClone dos LUNs. Cópias FlexClone de LUNs são legíveis e graváveis.

O que você vai precisar

Uma licença FlexClone deve ser instalada. Esta licença está incluída no "ONTAP One".

Sobre esta tarefa

O LUN FlexClone herda o atributo de reservas de espaço do LUN pai. Um LUN FlexClone reservado com espaço requer tanto espaço quanto o LUN pai reservado com espaço. Se o LUN FlexClone não estiver reservado com espaço, o volume deverá ter espaço suficiente para acomodar alterações no clone.

Passos

1. Verifique se o LUN não está mapeado ou a ser gravado.
2. Crie uma cópia Snapshot do volume que contém os LUNs:

   ```
   volume snapshot create -vserver vserver_name -volume volume_name -snapshot
   snapshot_name
   ```

   Você deve criar uma cópia Snapshot (a cópia Snapshot de backup) do LUN que deseja clonar.

3. Crie o LUN FlexClone a partir da cópia Snapshot:

   ```
   file clone create -vserver vserver_name -volume volume_name -source-path
   ```

source_path -snapshot-name *snapshot_name* -destination-path *destination_path*

Se você precisar que o LUN FlexClone esteja disponível para exclusão automática, inclua `-autodelete true`o . Se você estiver criando esse LUN FlexClone em um volume usando provisionamento semi-espesso, será necessário habilitar a exclusão automática para todos os LUNs FlexClone.

4. Verifique se o LUN FlexClone está correto:

   `lun show -vserver *vserver_name*`

```
Vserver Path                      State    Mapped    Type     Size
------- ----------------------    -------- --------- -------- -------
vs1     /vol/vol1/lun1_clone      online   unmapped windows   47.07MB
vs1     /vol/vol1/lun1_snap_clone online   unmapped windows   47.07MB
```

Impedir a eliminação automática de um ficheiro FlexClone ou LUN FlexClone

Se você configurar um FlexVol volume para excluir automaticamente arquivos FlexClone e LUNs FlexClone, qualquer clone que atenda aos critérios especificados poderá ser excluído. Se você tiver arquivos FlexClone ou LUNs FlexClone específicos que deseja preservar, poderá excluí-los do processo de exclusão automática do FlexClone.

Antes de começar

Uma licença FlexClone deve ser instalada. Esta licença está incluída no "ONTAP One".

Sobre esta tarefa

Quando você cria um arquivo FlexClone ou LUN FlexClone, por padrão, a configuração de ciclo de vida para o clone é desativada. Os arquivos do FlexClone e os LUNs do FlexClone com o recurso de configuração de ciclo de vida desativado são preservados quando você configura um FlexVol volume para excluir automaticamente clones para recuperar espaço no volume.

> Se você definir o `commitment` nível no volume como `try` ou `disrupt`, poderá preservar individualmente arquivos FlexClone ou LUNs FlexClone específicos desativando o modo de exibição de dados para esses clones. No entanto, se você definir o `commitment` nível no volume como `destroy` e as listas destruir incluir `lun_clone,file_clone`, a configuração de volume substituirá a configuração clone e todos os arquivos FlexClone e FlexClone LUNs poderão ser excluídos independentemente da configuração de ciclo de vida dos clones.

Passos

1. Evite que um arquivo FlexClone específico ou LUN FlexClone seja excluído automaticamente usando o `volume file clone autodelete` comando.

   O exemplo a seguir mostra como você pode desativar o FlexClone LUN lun1_clone contido no vol1:

```
cluster1::> volume file clone autodelete -vserver vs1 -volume vol1
-clone-path lun1_clone -enable false
```

Um arquivo ou LUN FlexClone com o sistema de diagnóstico guiado por sintomas (FlexClone) desativado não pode ser excluído automaticamente para recuperar espaço no volume.

2. Verifique se o arquivo FlexClone ou FlexClone LUN está desabilitado usando o `volume file clone show-autodelete` comando.

   O exemplo a seguir mostra que o FlexClone lun lun1_clone é falso:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path
vol/vol1/lun1_clone
                                                                Vserver
Name: vs1
                                                                Clone Path:
vol/vol1/lun1_clone
                                                                Autodelete
Enabled: false
```

Configurar e usar backups do SnapVault em um ambiente SAN

Configure e use backups do SnapVault em uma visão geral do ambiente SAN

A configuração e o uso do SnapVault em um ambiente SAN são muito semelhantes à configuração e ao uso em um ambiente nas, mas a restauração de LUNs em um ambiente SAN requer alguns procedimentos especiais.

Os backups do SnapVault contêm um conjunto de cópias somente leitura de um volume de origem. Em um ambiente SAN, você sempre faz backup de volumes inteiros para o volume secundário do SnapVault, e não LUNs individuais.

O procedimento para criar e inicializar a relação SnapVault entre um volume primário que contém LUNs e um volume secundário que atua como um backup do SnapVault é idêntico ao procedimento usado com volumes FlexVol usados para protocolos de arquivo. Este procedimento é descrito em pormenor em "Proteção de dados".

É importante garantir que o backup de LUNs que estão sendo feitos estejam em um estado consistente antes que as cópias Snapshot sejam criadas e copiadas para o volume secundário do SnapVault. A automação da criação de cópias Snapshot com o SnapCenter garante que os LUNs de backup sejam completos e utilizáveis pela aplicação original.

Há três opções básicas para restaurar LUNs de um volume secundário do SnapVault:

- Você pode mapear um LUN diretamente do volume secundário do SnapVault e conetar um host ao LUN para acessar o conteúdo do LUN.

  O LUN é somente leitura e você pode mapear apenas a partir da cópia Snapshot mais recente no backup do SnapVault. Reservas persistentes e outros metadados LUN são perdidos. Se desejar, você pode usar um programa de cópia no host para copiar o conteúdo do LUN de volta para o LUN original, se ele ainda estiver acessível.

  O LUN tem um número de série diferente do LUN de origem.

- Você pode clonar qualquer cópia Snapshot no volume secundário do SnapVault para um novo volume de leitura-gravação.

  Em seguida, é possível mapear qualquer um dos LUNs no volume e conetar um host ao LUN para acessar o conteúdo do LUN. Se desejar, você pode usar um programa de cópia no host para copiar o conteúdo do LUN de volta para o LUN original, se ele ainda estiver acessível.

- Você pode restaurar todo o volume que contém o LUN de qualquer cópia Snapshot no volume secundário do SnapVault.

  A restauração de todo o volume substitui todos os LUNs e quaisquer arquivos no volume. Todos os novos LUNs criados desde a criação da cópia Snapshot são perdidos.

  Os LUNs retêm seu mapeamento, números de série, UUIDs e reservas persistentes.

Acesse uma cópia LUN somente leitura a partir de um backup do SnapVault

Você pode acessar uma cópia somente leitura de um LUN a partir da cópia Snapshot mais recente em um backup do SnapVault. O ID do LUN, o caminho e o número de série são diferentes do LUN de origem e devem primeiro ser mapeados. Reservas persistentes, mapeamentos de LUN e grupos não são replicados para o volume secundário do SnapVault.

O que você vai precisar

- A relação SnapVault deve ser inicializada e a cópia Snapshot mais recente no volume secundário do SnapVault deve conter o LUN desejado.
- A máquina virtual de storage (SVM) que contém o backup do SnapVault deve ter uma ou mais LIFs com o protocolo SAN desejado acessível a partir do host usado para acessar a cópia LUN.
- Se você planeja acessar cópias LUN diretamente do volume secundário do SnapVault, crie seus grupos no SnapVault SVM com antecedência.

  Você pode acessar um LUN diretamente do volume secundário do SnapVault sem precisar primeiro restaurar ou clonar o volume que contém o LUN.

Sobre esta tarefa

Se uma nova cópia Snapshot for adicionada ao volume secundário do SnapVault enquanto você tiver um LUN mapeado de uma cópia Snapshot anterior, o conteúdo do LUN mapeado será alterado. O LUN ainda é mapeado com os mesmos identificadores, mas os dados são retirados da nova cópia Snapshot. Se o tamanho do LUN mudar, alguns hosts detetarão automaticamente a alteração de tamanho; os hosts do Windows exigem uma nova varredura de disco para pegar qualquer alteração de tamanho.

Passos

1. Execute o `lun show` comando para listar os LUNs disponíveis no volume secundário do SnapVault.

   Neste exemplo, você pode ver os LUNs originais no volume primário srcvolA e as cópias no volume secundário do SnapVault dstvolB:

```
cluster::> lun show

Vserver   Path                State   Mapped   Type          Size
--------  ------------------  ------  -------  --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

2. Se o igrop para o host desejado ainda não existir no SVM que contém o volume secundário do SnapVault, execute o `igroup create` comando para criar um igrop.

   Este comando cria um grupo para um host do Windows que usa o protocolo iSCSI:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

3. Execute o `lun mapping create` comando para mapear a cópia LUN desejada para o igroup.

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A
  -igroup temp_igroup
```

4. Conete o host ao LUN e acesse o conteúdo do LUN conforme desejado.

Restaure um único LUN a partir de um backup do SnapVault

Você pode restaurar um único LUN para um novo local ou para o local original. Você pode restaurar a partir de qualquer cópia Snapshot no volume secundário do SnapVault. Para restaurar o LUN para o local original, primeiro restaure-o para um novo local e, em seguida, copie-o.

O que você vai precisar

- A relação do SnapVault deve ser inicializada e o volume secundário do SnapVault deve conter uma cópia Snapshot apropriada para ser restaurada.
- A máquina virtual de storage (SVM) que contém o volume secundário do SnapVault deve ter uma ou mais LIFs com o protocolo SAN desejado que podem ser acessados pelo host usado para acessar a cópia LUN.
- Os grupos já devem existir no SnapVault SVM.

Sobre esta tarefa

O processo inclui a criação de um clone de volume de leitura e gravação a partir de uma cópia Snapshot no volume secundário do SnapVault. Você pode usar o LUN diretamente do clone ou, opcionalmente, copiar o conteúdo do LUN de volta para o local original do LUN.

O LUN no clone tem um caminho e um número de série diferentes do LUN original. Reservas persistentes não são retidas.

Passos

1. Execute o `snapmirror show` comando para verificar o volume secundário que contém o backup do SnapVault.

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                        Snapmirrored
                                Idle       -         true    -
```

2. Execute o `volume snapshot show` comando para identificar a cópia Snapshot da qual você deseja restaurar o LUN.

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

3. Execute o `volume clone create` comando para criar um clone de leitura e gravação a partir da cópia Snapshot desejada.

   O clone de volume é criado no mesmo agregado que o backup do SnapVault. Deve haver espaço suficiente no agregado para armazenar o clone.

```
cluster::> volume clone create -vserver vserverB
  -flexclone dstvolB_clone -type RW -parent-volume dstvolB
  -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. Execute o `lun show` comando para listar os LUNs no clone de volume.

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone

Vserver   Path                      State   Mapped   Type
--------- ------------------------  ------- -------- --------
vserverB  /vol/dstvolB_clone/lun_A  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_B  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_C  online  unmapped windows

3 entries were displayed.
```

5. Se o igrop para o host desejado ainda não existir no SVM que contém o backup do SnapVault, execute o `igroup create` comando para criar um igrop.

   Este exemplo cria um grupo para um host do Windows que usa o protocolo iSCSI:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

6. Execute o `lun mapping create` comando para mapear a cópia LUN desejada para o igroup.

```
cluster::> lun mapping create -vserver vserverB
  -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

7. Conete o host ao LUN e acesse o conteúdo do LUN, conforme desejado.

   O LUN é leitura-escrita e pode ser usado no lugar do LUN original. Como o número de série do LUN é diferente, o host o interpreta como um LUN diferente do original.

8. Use um programa de cópia no host para copiar o conteúdo do LUN de volta para o LUN original.

Restaurar todos os LUNs em um volume a partir de um backup do SnapVault

Se um ou mais LUNs em um volume precisarem ser restaurados a partir de um backup do SnapVault, você poderá restaurar todo o volume. A restauração do volume afeta todos os LUNs no volume.

O que você vai precisar

A relação do SnapVault deve ser inicializada e o volume secundário do SnapVault deve conter uma cópia Snapshot apropriada para ser restaurada.

Sobre esta tarefa

Restaurar um volume inteiro retorna o volume ao estado em que estava quando a cópia Snapshot foi feita. Se um LUN foi adicionado ao volume após a cópia Snapshot, esse LUN será removido durante o processo de

restauração.

Depois de restaurar o volume, os LUNs permanecem mapeados para os grupos para os quais foram mapeados pouco antes da restauração. O mapeamento LUN pode ser diferente do mapeamento no momento da cópia Snapshot. Reservas persistentes nas LUNs dos clusters de host são retidas.

Passos

1. Pare a e/S para todos os LUNs no volume.
2. Execute o `snapmirror show` comando para verificar o volume secundário que contém o volume secundário do SnapVault.

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                        Snapmirrored
                                Idle       -         true    -
```

3. Execute o `volume snapshot show` comando para identificar a cópia Snapshot da qual você deseja restaurar.

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

4. Execute o `snapmirror restore` comando e especifique a `-source-snapshot` opção para especificar a cópia Snapshot a ser usada.

   O destino especificado para a restauração é o volume original para o qual você está restaurando.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. Se você estiver compartilhando LUNs em um cluster de host, restaure as reservas persistentes nos LUNs dos hosts afetados.

Restaurar um volume a partir de uma cópia de segurança do SnapVault

No exemplo a seguir, o LUN chamado LUN_D foi adicionado ao volume depois que a cópia Snapshot foi criada. Depois de restaurar todo o volume da cópia Snapshot, lun_D não aparece mais.

Na `lun show` saída do comando, você pode ver os LUNs no volume primário srcvolA e as cópias somente leitura desses LUNs no volume secundário do SnapVault dstvolB. Não há cópia de lun_D no backup do SnapVault.

```
cluster::> lun show
Vserver   Path                 State   Mapped   Type          Size
--------- ------------------   ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_D  online  mapped   windows  250.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

7 entries were displayed.

cluster::>snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB
  -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205
on volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.

cluster::> lun show
Vserver   Path                 State   Mapped   Type          Size
--------- ------------------   ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

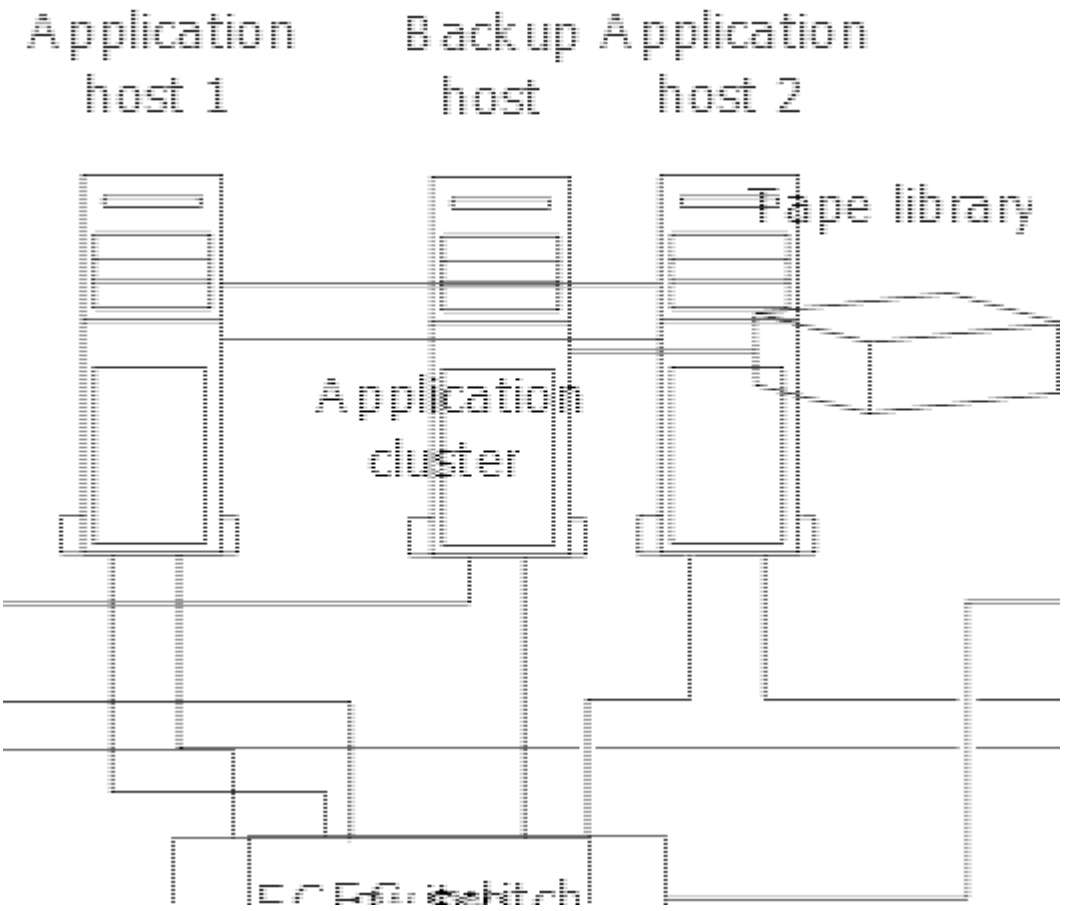
Depois que o volume é restaurado a partir do volume secundário do SnapVault, o volume de origem não contém mais lun_D. Não é necessário remapear novamente os LUNs no volume de origem após a restauração, pois eles ainda estão mapeados.

Como conetar um sistema de backup de host ao sistema de storage primário

É possível fazer backup de sistemas SAN na fita por meio de um host de backup separado para evitar a degradação da performance no host do aplicativo.

É imperativo que você mantenha os dados SAN e nas separados para fins de backup. A figura abaixo mostra a configuração física recomendada para um sistema de backup do host para o sistema de storage primário.

Você deve configurar volumes como somente SAN. Os LUNs podem ser confinados a um único volume ou os LUNs podem ser espalhados por vários volumes ou sistemas de armazenamento.



Os volumes em um host podem consistir em um único LUN mapeado a partir do sistema de armazenamento ou vários LUNs usando um gerenciador de volumes, como VxVM em sistemas HP-UX.

Faça backup de um LUN por meio de um sistema de backup de host

Você pode usar um LUN clonado de uma cópia Snapshot como dados de origem para o sistema de backup do host.

O que você vai precisar

Um LUN de produção deve existir e ser mapeado para um grupo que inclua o nome do nó WWPN ou iniciador do servidor de aplicativos. O LUN também deve ser formatado e acessível ao host

Passos

1. Salve o conteúdo dos buffers do sistema de arquivos host no disco.

   Você pode usar o comando fornecido pelo seu sistema operacional host ou usar o SnapDrive para Windows ou SnapDrive para UNIX. Você também pode optar por fazer desta etapa parte do script de pré-processamento de backup SAN.

2. Use o `volume snapshot create` comando para criar uma cópia Snapshot do LUN de produção.

   ```
   volume snapshot create -vserver vs0 -volume vol3 -snapshot vol3_snapshot
   -comment "Single snapshot" -foreground false
   ```

3. Use o `volume file clone create` comando para criar um clone do LUN de produção.

   ```
   volume file clone create -vserver vs3 -volume vol3 -source-path lun1 -snapshot
   -name snap_vol3 -destination-path lun1_backup
   ```

4. Use o `lun igroup create` comando para criar um grupo que inclua o WWPN do servidor de backup.

   ```
   lun igroup create -vserver vs3 -igroup igroup3 -protocol fc -ostype windows
   -initiator 10:00:00:00:c9:73:5b:91
   ```

5. Use o `lun mapping create` comando para mapear o clone LUN que você criou na Etapa 3 para o host de backup.

   ```
   lun mapping create -vserver vs3 -volume vol3 -lun lun1_backup -igroup igroup3
   ```

   Você pode optar por fazer desta etapa parte do script de pós-processamento do aplicativo de backup SAN.

6. A partir do host, descubra o novo LUN e disponibilize o sistema de arquivos para o host.

   Você pode optar por fazer desta etapa parte do script de pós-processamento do aplicativo de backup SAN.

7. Faça backup dos dados no clone LUN do host de backup para fita usando seu aplicativo de backup SAN.
8. Use o `lun modify` comando para colocar o clone LUN off-line.

   ```
   lun modify -vserver vs3 -path /vol/vol3/lun1_backup -state offline
   ```

9. Utilize o `lun delete` para remover o clone LUN.

   ```
   lun delete -vserver vs3 -volume vol3 -lun lun1_backup
   ```

10. Use o `volume snapshot delete` comando para remover a cópia Snapshot.

    ```
    volume snapshot delete -vserver vs3 -volume vol3 -snapshot vol3_snapshot
    ```

Referência de configuração SAN

Visão geral da configuração SAN

Uma rede de área de storage (SAN) consiste em uma solução de storage conetada a hosts por meio de um protocolo de transporte SAN, como iSCSI ou FC. Você pode configurar sua SAN para que sua solução de armazenamento seja conetada aos hosts por meio de um ou mais switches. Se você estiver usando iSCSI, também poderá configurar sua SAN para que sua solução de armazenamento seja conetada diretamente ao host sem usar um switch.

Em uma SAN, vários hosts, usando sistemas operacionais diferentes, como Windows, Linux ou UNIX, podem acessar a solução de storage ao mesmo tempo. Você pode usar "Mapeamento LUN seletivo" e "portsets" para limitar o acesso aos dados entre os hosts e o armazenamento.

Para iSCSI, a topologia de rede entre a solução de armazenamento e os hosts é chamada de rede. Para FC, FC/NVMe e FCoE, a topologia de rede entre a solução de storage e os hosts é conhecida como malha. Para criar redundância, que o protege contra a perda de acesso aos dados, você deve configurar sua SAN com pares de HA em uma configuração de várias redes ou várias estruturas. Configurações que usam nós únicos ou redes/malhas únicas não são totalmente redundantes, portanto não são recomendadas.

Depois de configurar a SAN, pode "Provisionar storage para iSCSI ou FC"ou pode "Provisionar storage para FC/NVMe". Então você pode se conetar aos seus hosts para começar a prestar serviços de dados.

O suporte ao protocolo SAN varia de acordo com sua versão do ONTAP, sua plataforma e sua configuração. Para obter detalhes sobre sua configuração específica, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Informações relacionadas

- "Visão geral da administração DE SAN"
- "Configuração, suporte e limitações do NVMe"

Configurações iSCSI

Maneiras de configurar hosts SAN iSCSI

Você deve configurar sua configuração iSCSI com pares de alta disponibilidade (HA) que se conetam diretamente aos hosts SAN iSCSI ou que se conetam aos hosts por meio de um ou mais switches IP.

"Pares HA" São definidos como os nós de relatório para os caminhos Ativo/otimizado e Ativo/Unoptimized que serão usados pelos hosts para acessar os LUNs. Vários hosts, usando sistemas operacionais diferentes, como Windows, Linux ou UNIX, podem acessar o storage ao mesmo tempo. Os hosts exigem que uma solução de multipathing suportada que suporte ALUA seja instalada e configurada. Sistemas operacionais suportados e soluções multipathing podem ser verificados no "Ferramenta de Matriz de interoperabilidade do NetApp".

Em uma configuração de várias redes, há dois ou mais switches conetando os hosts ao sistema de armazenamento. As configurações de várias redes são recomendadas porque são totalmente redundantes. Em uma configuração de rede única, há um switch conetando os hosts ao sistema de armazenamento. As configurações de rede única não são totalmente redundantes.

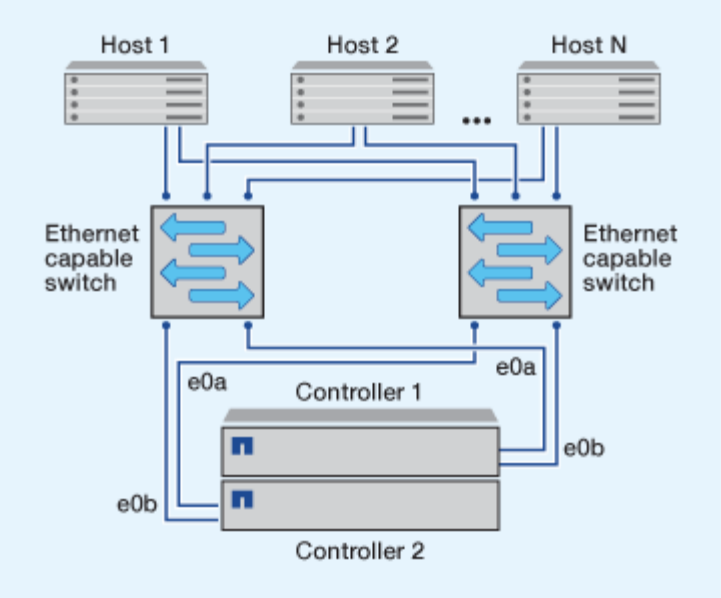
> "Configurações de nó único" não são recomendadas porque não fornecem a redundância necessária para dar suporte à tolerância de falhas e operações ininterruptas.

Informações relacionadas

- Saiba como "Mapeamento LUN seletivo (SLM)" limita os caminhos utilizados para acessar as LUNs de propriedade de um par de HA.
- Saiba mais "SAN LIFs"sobre .
- Saiba mais sobre o "Benefícios das VLANs no iSCSI".

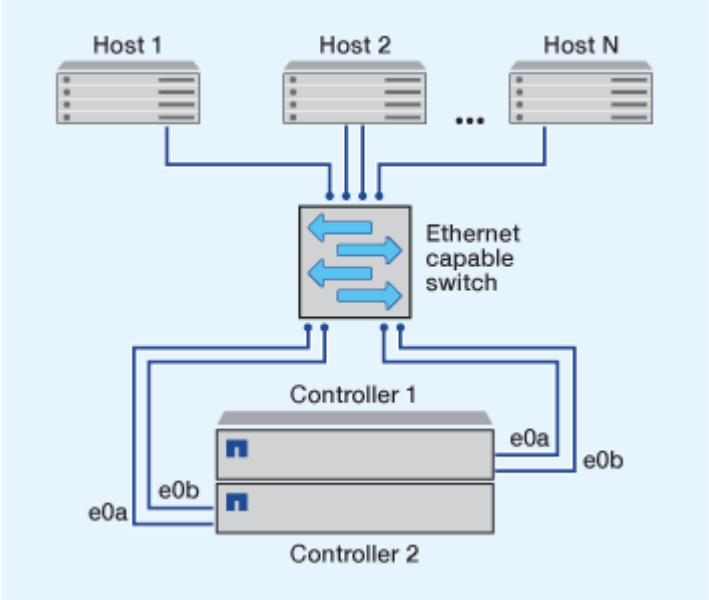
Configurações iSCSI de várias redes

Em configurações de par de HA com várias redes, dois ou mais switches conetam o par de HA a um ou mais hosts. Como existem vários switches, essa configuração é totalmente redundante.



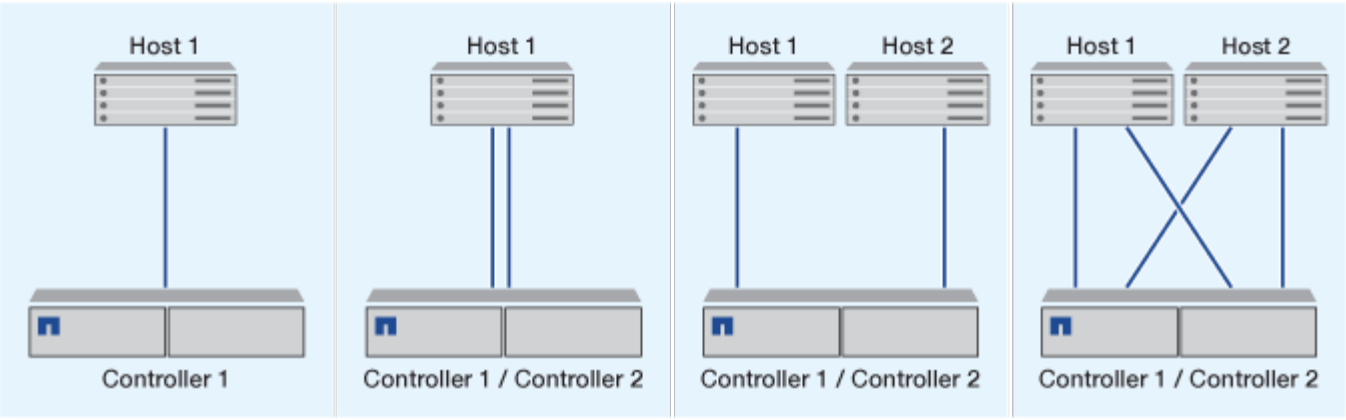
Configurações iSCSI de rede única

Nas configurações de par de HA de rede única, um switch conecta o par de HA a um ou mais hosts. Como há um único switch, essa configuração não é totalmente redundante.



Configuração iSCSI de ligação direta

Em uma configuração com conexão direta, um ou mais hosts são conetados diretamente aos controladores.



Benefícios de usar VLANs em configurações iSCSI

Uma VLAN consiste em um grupo de portas de switch agrupadas em um domínio de broadcast. Uma VLAN pode estar em um único switch ou pode abranger vários chassis de switch. As VLANs estáticas e dinâmicas permitem aumentar a segurança, isolar problemas e limitar os caminhos disponíveis na infraestrutura de rede IP.

Ao implementar VLANs em grandes infraestruturas de rede IP, você obtém os seguintes benefícios:

- Maior segurança.

  As VLANs permitem que você aproveite a infra-estrutura existente e ainda forneça segurança aprimorada, pois limitam o acesso entre diferentes nós de uma rede Ethernet ou uma SAN IP.

- Maior confiabilidade da rede Ethernet e da SAN IP ao isolar problemas.
- Redução do tempo de resolução de problemas limitando o espaço do problema.
- Redução do número de caminhos disponíveis para uma porta de destino iSCSI específica.
- Redução do número máximo de caminhos usados por um host.

  Ter muitos caminhos retarda os tempos de reconexão. Se um host não tiver uma solução multipathing, você poderá usar VLANs para permitir apenas um caminho.

VLANs dinâmicas

As VLANs dinâmicas são baseadas em endereços MAC. Você pode definir uma VLAN especificando o endereço MAC dos membros que deseja incluir.

As VLANs dinâmicas fornecem flexibilidade e não exigem mapeamento para as portas físicas onde o dispositivo está fisicamente conetado ao switch. Você pode mover um cabo de uma porta para outra sem reconfigurar a VLAN.

VLANs estáticas

As VLANs estáticas são baseadas em portas. O switch e a porta do switch são usados para definir a VLAN e seus membros.

As VLANs estáticas oferecem segurança aprimorada porque não é possível violar VLANs usando spoofing de controle de acesso de Mídia (MAC). No entanto, se alguém tiver acesso físico ao switch, substituir um cabo e reconfigurar o endereço de rede poderá permitir o acesso.

Em alguns ambientes, é mais fácil criar e gerenciar VLANs estáticas do que VLANs dinâmicas. Isso ocorre porque as VLANs estáticas exigem que somente o switch e o identificador de porta sejam especificados, em vez do endereço MAC de 48 bits. Além disso, você pode rotular intervalos de portas do switch com o identificador VLAN.

Configurações de FC

Maneiras de configurar hosts SAN FC e FC-NVMe

É recomendável configurar seus hosts SAN FC e FC-NVMe usando pares de HA e no mínimo dois switches. Isso fornece redundância nas camadas de malha e sistema de storage para dar suporte a tolerância de falhas e operações ininterruptas. Você não pode conectar diretamente hosts SAN FC ou FC-NVMe a pares de HA sem usar um switch.

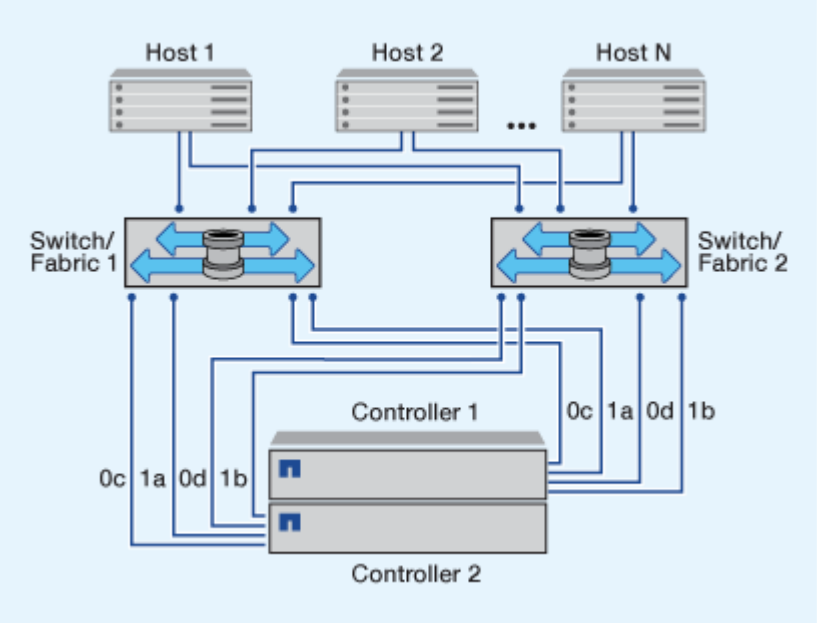
Cascata, malha parcial, malha completa, borda central e tecidos diretor são todos métodos padrão do setor de conexão de switches FC a uma malha e todos são compatíveis. O uso de malhas de switch FC heterogêneas não é suportado, exceto no caso de switches blade incorporados. Exceções específicas estão listadas no "Ferramenta de Matriz de interoperabilidade". Uma malha pode consistir em um ou vários switches, e os controladores de storage podem ser conectados a vários switches.

Vários hosts, usando sistemas operacionais diferentes, como Windows, Linux ou UNIX, podem acessar os controladores de storage ao mesmo tempo. Os hosts exigem que uma solução de multipathing suportada seja instalada e configurada. Sistemas operacionais suportados e soluções multipathing podem ser verificados na ferramenta Matriz de interoperabilidade.

Configurações MultiFabric FC e FC-NVMe

Nas configurações de par de HA com várias malhas, há dois ou mais switches que conectam pares de HA a um ou mais hosts. Para simplificar, a figura a seguir de par de HA com várias malhas mostra apenas duas malhas, mas você pode ter duas ou mais malhas em qualquer configuração de várias malhas.

Os números de porta de destino FC (0C, 0d, 1a, 1b) nas ilustrações são exemplos. Os números reais das portas variam dependendo do modelo do nó de armazenamento e se você está usando adaptadores de expansão.

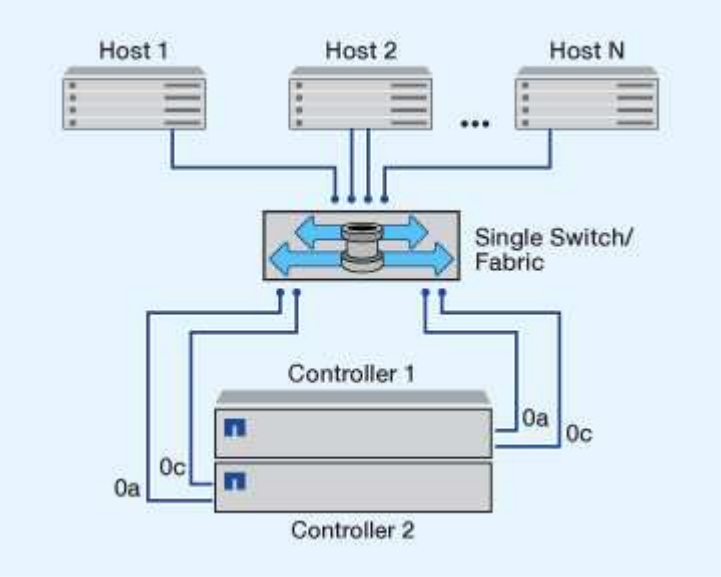


Configurações FC de malha única e FC-NVMe

Nas configurações de par de HA de estrutura única, há uma malha que conecta ambas as controladoras no par de HA a um ou mais hosts. Como os hosts e as controladoras são conectados por meio de um único switch, as configurações de par de HA de estrutura única não são totalmente redundantes.

Os números de porta de destino FC (0a, 0C) nas ilustrações são exemplos. Os números reais das portas variam dependendo do modelo do nó de armazenamento e se você está usando adaptadores de expansão.

Todas as plataformas compatíveis com configurações de FC são compatíveis com configurações de par de HA de malha única.



"Configurações de nó único" não são recomendadas porque não fornecem a redundância necessária para dar suporte à tolerância de falhas e operações ininterruptas.

Informações relacionadas

- Saiba como "Mapeamento LUN seletivo (SLM)" limita os caminhos utilizados para acessar as LUNs de propriedade de um par de HA.
- Saiba mais "SAN LIFs"sobre .

Práticas recomendadas de configuração de switch FC

Para obter o melhor desempenho, você deve considerar certas práticas recomendadas ao configurar seu switch FC.

Uma configuração de velocidade de link fixo é a prática recomendada para configurações de switch FC, especialmente para malhas grandes, porque fornece o melhor desempenho para recompilações de malha e pode economizar tempo de maneira significativa. Embora a negociação automática forneça a maior flexibilidade, a configuração do switch FC nem sempre funciona conforme o esperado e adiciona tempo à sequência geral de construção da malha.

Todos os switches que estão conetados à malha devem suportar a virtualização N_Port ID (NPIV) e devem ter o NPIV habilitado. O ONTAP usa NPIV para apresentar metas FC em uma malha.

Para obter detalhes sobre quais ambientes são suportados, consulte o "Ferramenta de Matriz de

interoperabilidade do NetApp".

Para obter as práticas recomendadas de FC e iSCSI, "Relatório técnico da NetApp 4080: Práticas recomendadas para SAN moderna" consulte .

Número suportado de contagens de saltos FC

A contagem máxima de FC HOP suportada entre um host e um sistema de storage depende do fornecedor do switch e do suporte do sistema de storage para configurações FC.

A contagem de saltos é definida como o número de switches no caminho entre o iniciador (host) e o destino (sistema de armazenamento). Cisco também se refere a esse valor como o *diâmetro da malha SAN*.

Fornecedor do interrutor	Contagem de saltos suportada
Brocade	7 para FC, 5 para FCoE
Cisco	7 para FC, até 3 dos switches podem ser switches FCoE.

Informações relacionadas

"Downloads do NetApp: Documentos da matriz de escalabilidade do Brocade"

"Downloads do NetApp: Documentos da matriz de escalabilidade do Cisco"

Recomendações de configuração de porta de destino FC

As portas de destino FC podem ser configuradas e usadas no protocolo FC-NVMe da mesma maneira que são configuradas e usadas no protocolo FC. O suporte ao protocolo FC-NVMe varia de acordo com a sua plataforma e a versão do ONTAP. Use o NetApp Hardware Universe para verificar o suporte.

Para obter o melhor desempenho e a mais alta disponibilidade, você deve usar a configuração de porta de destino recomendada listada na "NetApp Hardware Universe" para sua plataforma específica.

Configuração para portas de destino FC com ASICs compartilhados

As plataformas a seguir têm pares de portas com circuitos integrados (ASICs) específicos de aplicativos compartilhados. Se você usar um adaptador de expansão com essas plataformas, configure suas portas FC para que elas não usem o mesmo ASIC para conetividade.

Controlador	Pares de portas com ASIC partilhado	Número de portas de destino: Portas recomendadas
• FAS8200 • AFF A300	0g-0h	1: 0g 2: 0g, 0h

Controlador	Pares de portas com ASIC partilhado	Número de portas de destino: Portas recomendadas
• FAS2720 • FAS2750 • AFF A220	0c-0d 0e-0f	1: 0c 2: 0c, 0e 3: 0c, 0e, 0d 4: 0c, 0e, 0d, 0f

Velocidades compatíveis com porta de destino FC

As portas de destino FC podem ser configuradas para serem executadas em diferentes velocidades. Todas as portas de destino usadas por um determinado host devem ser definidas para a mesma velocidade. Você deve definir a velocidade da porta de destino para corresponder à velocidade do dispositivo ao qual ela se coneta. Não use a negociação automática para a velocidade da porta. Uma porta definida como negociação automática pode levar mais tempo para se reconetar após uma tomada de controle/giveback ou outra interrupção.

É possível configurar portas integradas e adaptadores de expansão para serem executados nas seguintes velocidades. Cada porta do controlador e adaptador de expansão pode ser configurada individualmente para diferentes velocidades, conforme necessário.

Portas de 4 GB	Portas de 8 GB	Portas de 16 GB	Portas de 32 GB
• 4 GB • 2 GB • 1 GB	• 8 GB • 4 GB • 2 GB	• 16 GB • 8 GB • 4 GB	• 32 GB • 16 GB • 8 GB

As portas UTA2 podem usar um adaptador SFP de 8 GB para suportar velocidades de 8, 4 e 2 GB, se necessário.

Gerenciar sistemas com adaptadores FC

Visão geral do gerenciamento de sistemas com adaptadores FC

Os comandos estão disponíveis para gerenciar adaptadores FC integrados e placas adaptadoras FC. Esses comandos podem ser usados para configurar o modo do adaptador, exibir informações do adaptador e alterar a velocidade.

A maioria dos sistemas de storage tem adaptadores FC integrados que podem ser configurados como iniciadores ou destinos. Você também pode usar placas de adaptador FC configuradas como iniciadores ou destinos. Os iniciadores se conetam aos compartimentos de disco back-end e, possivelmente, a matrizes de armazenamento estranho (FlexArray). Os destinos se conetam apenas aos switches FC. Ambas as portas HBA de destino FC e a velocidade da porta do switch devem ser definidas para o mesmo valor e não devem ser definidas para auto.

Comandos para gerenciar adaptadores FC

Você pode usar comandos FC para gerenciar adaptadores de destino FC, adaptadores iniciadores FC e adaptadores FC integrados para o controlador de storage. Os mesmos comandos são usados para gerenciar adaptadores FC para o protocolo FC e o protocolo

FC-NVMe.

Os comandos do adaptador do iniciador FC funcionam apenas no nível do nó. Você deve usar o `run -node node_name` comando antes de usar os comandos do adaptador do iniciador FC.

Comandos para gerenciar adaptadores de destino FC

Se você quiser…	Use este comando…
Exibir as informações do adaptador FC em um nó	`network fcp adapter show`
Modifique os parâmetros do adaptador de destino FC	`network fcp adapter modify`
Apresentar informações de tráfego do protocolo FC	`run -node node_name sysstat -f`
Apresentar durante quanto tempo o protocolo FC foi executado	`run -node node_name uptime`
Exibir configuração e status do adaptador	`run -node node_name sysconfig -v adapter`
Verifique quais placas de expansão estão instaladas e se existem erros de configuração	`run -node node_name sysconfig -ac`
Exibir uma página de manual para um comando	`man command_name`

Comandos para gerenciar adaptadores de iniciador FC

Se você quiser…	Use este comando…
Exibir informações para todos os iniciadores e seus adaptadores em um nó	`run -node node_name storage show adapter`
Exibir configuração e status do adaptador	`run -node node_name sysconfig -v adapter`
Verifique quais placas de expansão estão instaladas e se existem erros de configuração	`run -node node_name sysconfig -ac`

Comandos para gerenciar adaptadores FC integrados

Se você quiser…	Use este comando…
Exibir o status das portas FC integradas	`system node hardware unified-connect show`

Configurar adaptadores FC para o modo iniciador

Você pode configurar portas FC individuais de adaptadores integrados e determinadas placas de adaptador FC para o modo iniciador. O modo iniciador é usado para conetar as portas a unidades de fita, bibliotecas de fita ou armazenamento de terceiros com virtualização FlexArray ou importação de LUN estrangeiro (FLI).

O que você vai precisar

- Os LIFs no adaptador devem ser removidos de quaisquer conjuntos de portas dos quais sejam membros.
- Todos os LIF de todas as máquinas virtuais de armazenamento (SVM) que usam a porta física a ser modificada devem ser migrados ou destruídos antes de alterar a personalidade da porta física de destino para iniciador.

Sobre esta tarefa

Cada porta FC integrada pode ser configurada individualmente como iniciador ou destino. As portas em certos adaptadores FC também podem ser configuradas individualmente como uma porta de destino ou uma porta de iniciador, assim como as portas FC integradas. Uma lista de adaptadores que podem ser configurados para o modo de destino está disponível no "NetApp Hardware Universe".

O NVMe/FC oferece suporte ao modo iniciador.

Passos

1. Remova todas as LIFs do adaptador:

   `network interface delete -vserver SVM_name -lif lif_name,lif_name`

2. Coloque o adaptador offline:

   `network fcp adapter modify -node node_name -adapter adapter_port -status-admin down`

   Se o adaptador não ficar offline, você também pode remover o cabo da porta apropriada do adaptador no sistema.

3. Altere o adaptador de destino para iniciador:

   `system hardware unified-connect modify -t initiator adapter_port`

4. Reinicie o nó que hospeda o adaptador que você alterou.
5. Verifique se as portas FC estão configuradas no estado correto para sua configuração:

   `system hardware unified-connect show`

6. Coloque o adaptador novamente online:

   `node run -node node_name storage enable adapter adapter_port`

Configurar adaptadores FC para o modo de destino

Você pode configurar portas FC individuais de adaptadores integrados e determinadas placas de adaptador FC para o modo de destino. O modo de destino é usado para

conetar as portas aos iniciadores FC.

Sobre esta tarefa

Cada porta FC integrada pode ser configurada individualmente como iniciador ou destino. As portas em certos adaptadores FC também podem ser configuradas individualmente como uma porta de destino ou uma porta de iniciador, assim como as portas FC integradas. Uma lista de adaptadores que podem ser configurados para o modo de destino está disponível no "NetApp Hardware Universe".

As mesmas etapas são usadas na configuração de adaptadores FC para o protocolo FC e para o protocolo FC-NVMe. No entanto, apenas certos adaptadores FC são compatíveis com FC-NVMe. Consulte "NetApp Hardware Universe" a para obter uma lista de adaptadores compatíveis com o protocolo FC-NVMe.

Passos

1. Coloque o adaptador offline:

   `node run -node` *`node_name`* `storage disable adapter` *`adapter_name`*

   Se o adaptador não ficar offline, você também pode remover o cabo da porta apropriada do adaptador no sistema.

2. Altere o adaptador do iniciador para o destino:

   `system node hardware unified-connect modify -t target -node` *`node_name`* `adapter` *`adapter_name`*

3. Reinicie o nó que hospeda o adaptador que você alterou.
4. Verifique se a porta de destino tem a configuração correta:

   `network fcp adapter show -node` *`node_name`*

5. Coloque o adaptador online:

   `network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_port`* `-state up`

Exibir informações sobre um adaptador de destino FC

Você pode usar o `network fcp adapter show` comando para exibir as informações de configuração do sistema e do adaptador para qualquer adaptador FC no sistema.

Passo

1. Exiba informações sobre o adaptador FC usando o `network fcp adapter show` comando.

   A saída exibe informações de configuração do sistema e informações do adaptador para cada slot usado.

   `network fcp adapter show -instance -node node1 -adapter 0a`

Altere a velocidade do adaptador FC

Você deve definir a velocidade da porta de destino do adaptador para corresponder à velocidade do dispositivo ao qual ele se coneta, em vez de usar a negociação automática. Uma porta definida como negociação automática pode levar mais tempo

para se reconetar após uma tomada de controle/giveback ou outra interrupção.

O que você vai precisar

Todos os LIFs que usam esse adaptador como porta inicial devem estar offline.

Sobre esta tarefa

Como essa tarefa abrange todas as máquinas virtuais de armazenamento (SVMs) e todas as LIFs em um cluster, você deve usar os `-home-port` parâmetros e `-home-lif` para limitar o escopo dessa operação. Se você não usar esses parâmetros, a operação se aplica a todos os LIFs no cluster, o que pode não ser desejável.

Passos

1. Tire todos os LIFs neste adaptador offline:

   ```
   network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }
   -status-admin down
   ```

2. Coloque o adaptador offline:

   ```
   network fcp adapter modify -node node1 -adapter 0c -state down
   ```

   Se o adaptador não ficar offline, você também pode remover o cabo da porta apropriada do adaptador no sistema.

3. Determine a velocidade máxima do adaptador de porta:

   ```
   fcp adapter show -instance
   ```

   Não é possível modificar a velocidade do adaptador para além da velocidade máxima.

4. Alterar a velocidade do adaptador:

   ```
   network fcp adapter modify -node node1 -adapter 0c -speed 16
   ```

5. Coloque o adaptador online:

   ```
   network fcp adapter modify -node node1 -adapter 0c -state up
   ```

6. Coloque todos os LIFs no adaptador online:

   ```
   network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }
   -status-admin up
   ```

Portas FC compatíveis

O número de portas FC integradas e portas CNA/UTA2 configuradas para FC varia de acordo com o modelo da controladora. As portas FC também estão disponíveis por meio de adaptadores de expansão de destino FC compatíveis ou placas UTA2 adicionais configuradas com adaptadores FC SFP mais.

FC integrado, UTA e portas de UTA2 GbE

- As portas integradas podem ser configuradas individualmente como portas FC de destino ou iniciador.
- O número de portas FC integradas difere dependendo do modelo do controlador.

  O "NetApp Hardware Universe" contém uma lista completa de portas FC integradas em cada modelo de controladora.

- Os sistemas FAS2520 não são compatíveis com FC.

Portas FC do adaptador de expansão de destino

- Os adaptadores de expansão de destino disponíveis diferem dependendo do modelo do controlador.

  O "NetApp Hardware Universe" contém uma lista completa dos adaptadores de expansão de destino para cada modelo de controlador.

- As portas em alguns adaptadores de expansão FC são configuradas como iniciadores ou destinos na fábrica e não podem ser alteradas.

  Outras podem ser configuradas individualmente como portas FC de destino ou iniciador, assim como as portas FC integradas. Uma lista completa está disponível em "NetApp Hardware Universe".

Evite a perda de conetividade ao usar o adaptador X1133A-R6

Você pode evitar a perda de conetividade durante uma falha de porta configurando o sistema com caminhos redundantes para separar HBAs X1133A-R6.

O HBA X1133A-R6 é um adaptador FC de 4 portas e 16 GB que consiste em dois pares de 2 portas. O adaptador X1133A-R6 pode ser configurado como modo de destino ou modo de iniciador. Cada par de 2 portas é suportado por um único ASIC (por exemplo, porta 1 e porta 2 no ASIC 1 e porta 3 e porta 4 no ASIC 2). Ambas as portas em um único ASIC devem ser configuradas para operar no mesmo modo, seja no modo de destino ou no modo de iniciador. Se ocorrer um erro com o ASIC que suporta um par, ambas as portas do par ficam offline.

Para evitar essa perda de conetividade, configure o sistema com caminhos redundantes para separar HBAs X1133A-R6 ou com caminhos redundantes para portas compatíveis com ASICs diferentes no HBA.

Configurações FCoE

Maneiras de configurar a visão geral do FCoE

O FCoE pode ser configurado de várias maneiras usando switches FCoE. Configurações com conexão direta não são compatíveis com FCoE.

Todas as configurações FCoE são de estrutura dupla, totalmente redundantes e exigem software de multipathing no lado do host. Em todas as configurações FCoE, você pode ter vários switches FCoE e FC no caminho entre o iniciador e o destino, até o limite máximo de contagem de saltos. Para conetar switches entre si, os switches devem executar uma versão de firmware que suporte ISLs Ethernet. Cada host em qualquer configuração FCoE pode ser configurado com um sistema operacional diferente.

As configurações FCoE exigem switches Ethernet que suportam explicitamente os recursos FCoE. As configurações FCoE são validadas pelo mesmo processo de interoperabilidade e garantia de qualidade que

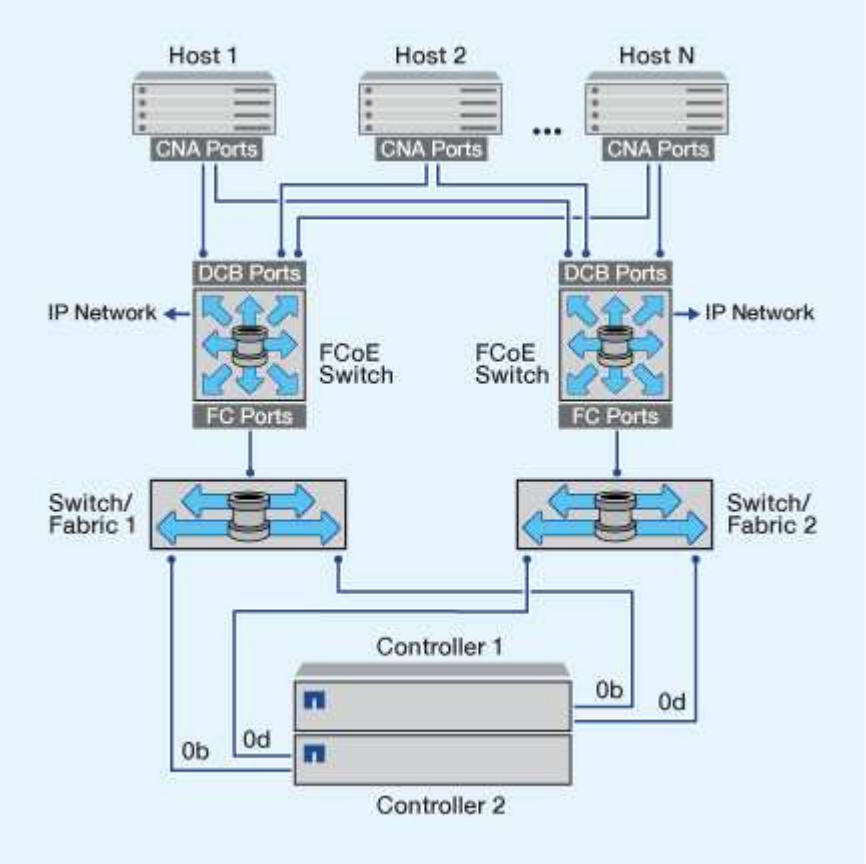
os switches FC. As configurações suportadas estão listadas na Matriz de interoperabilidade. Alguns dos parâmetros incluídos nessas configurações suportadas são o modelo de switch, o número de switches que podem ser implantados em uma única malha e a versão de firmware de switch suportada.

Os números da porta do adaptador de expansão de destino FC nas ilustrações são exemplos. Os números reais das portas podem variar, dependendo dos slots de expansão nos quais os adaptadores de expansão de destino FCoE estão instalados.

Iniciador FCoE para destino FC

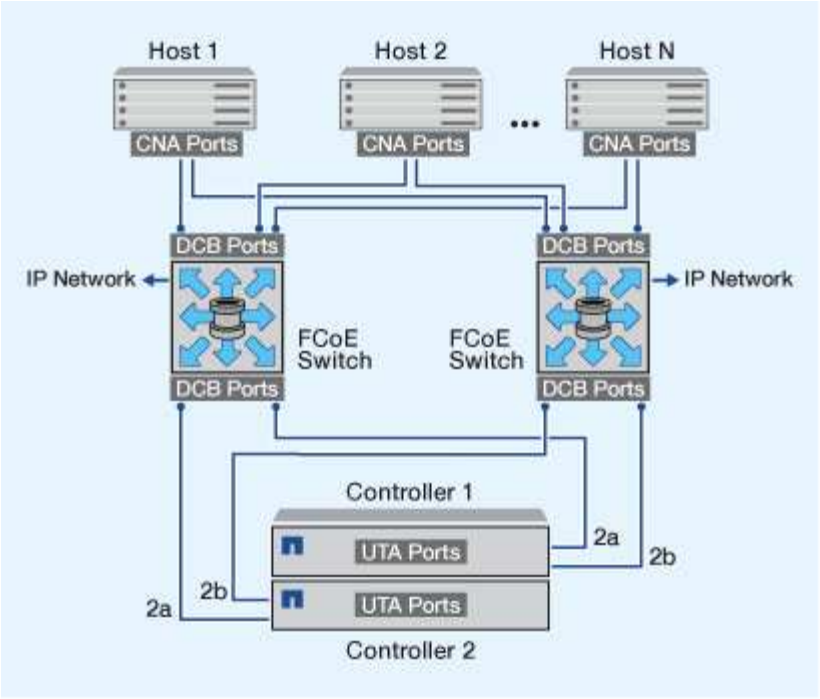
Usando os iniciadores FCoE (CNAs), você pode conetar hosts a ambos os controladores em um par de HA por meio de switches FCoE a portas de destino FC. O switch FCoE também deve ter portas FC. O iniciador FCoE do host sempre se coneta ao switch FCoE. O switch FCoE pode se conectar diretamente ao destino FC ou pode se conectar ao destino FC por meio de switches FC.

A ilustração a seguir mostra CNAs do host conetando-se a um switch FCoE e, em seguida, a um switch FC antes de se conetar ao par de HA:



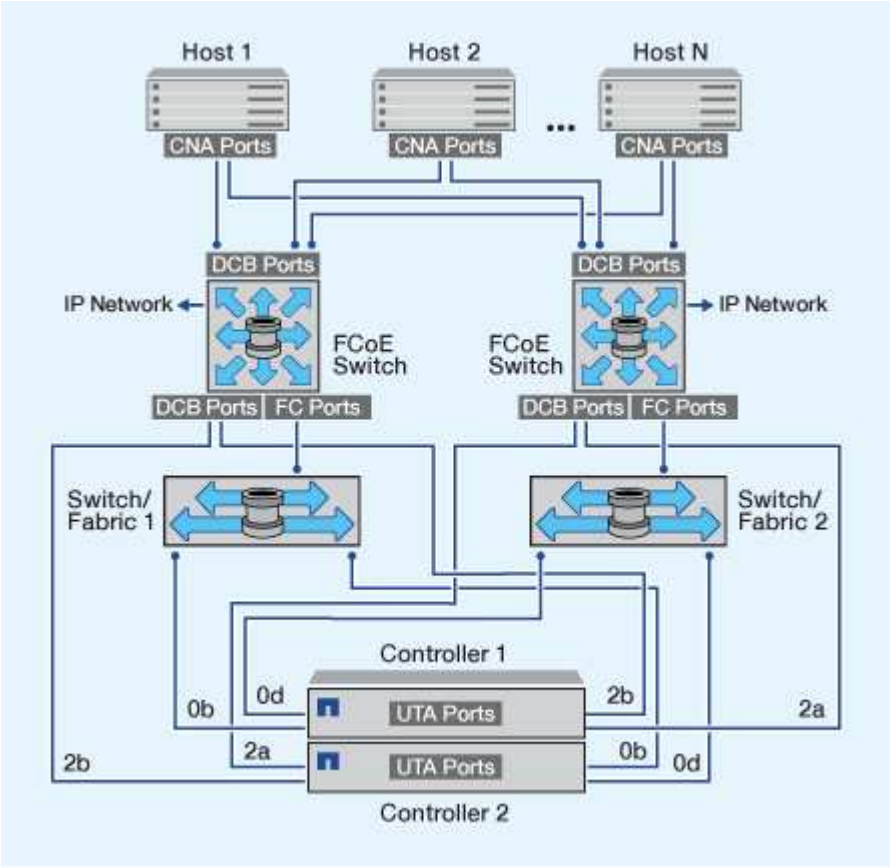
Iniciador FCoE para destino FCoE

Usando os iniciadores FCoE de host (CNAs), você pode conetar hosts a ambos os controladores em um par de HA a portas de destino FCoE (também chamadas de UTA ou UTA2s) por meio de switches FCoE.



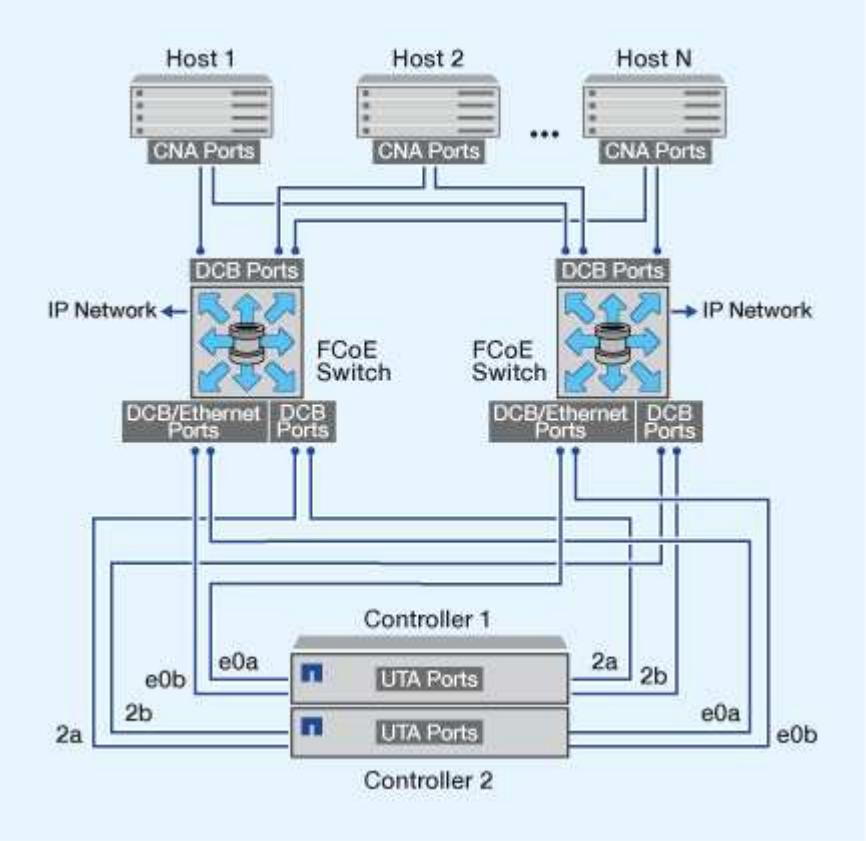
Iniciador FCoE para destinos FCoE e FC

Usando os iniciadores FCoE de host (CNAs), você pode conetar hosts a ambos os controladores em um par de HA a portas de destino FCoE e FC (também chamadas de UTA ou UTA2s) por meio de switches FCoE.



FCoE misturado com protocolos de storage IP

Usando os iniciadores FCoE de host (CNAs), você pode conetar hosts a ambos os controladores em um par de HA a portas de destino FCoE (também chamadas de UTA ou UTA2s) por meio de switches FCoE. As portas FCoE não podem usar a agregação de links tradicional a um único switch. Os switches Cisco suportam um tipo especial de agregação de links (Canal de porta virtual) que suporta FCoE. Um canal de porta virtual agrega links individuais a dois switches. Você também pode usar canais de porta virtual para outro tráfego Ethernet. As portas usadas para tráfego diferente do FCoE, incluindo NFS, SMB, iSCSI e outro tráfego Ethernet, podem usar portas Ethernet regulares nos switches FCoE.



Combinações de iniciador FCoE e destino

Certas combinações de iniciadores e destinos FC tradicionais e FCoE são suportadas.

Iniciadores FCoE

Você pode usar iniciadores FCoE em computadores host com destinos FCoE e FC tradicionais em controladores de armazenamento. O iniciador FCoE do host deve se conetar a um switch FCoE DCB (ponte de data center); a conexão direta a um destino não é suportada.

A tabela a seguir lista as combinações suportadas:

Iniciador	Alvo	Suportado?
FC	FC	Sim
FC	FCoE	Sim

Iniciador	Alvo	Suportado?
FCoE	FC	Sim
FCoE	FCoE	Sim

Destinos FCoE

É possível misturar portas de destino FCoE com portas FC de 4 GB, 8 GB ou 16 GB na controladora de storage, independentemente de as portas FC serem adaptadores de destino complementares ou portas integradas. Você pode ter adaptadores de destino FCoE e FC no mesmo controlador de storage.

As regras da combinação de portas FC integradas e de expansão ainda se aplicam.

Contagem de saltos com suporte para FCoE

A contagem máxima de saltos Fibre Channel over Ethernet (FCoE) suportada entre um host e um sistema de armazenamento depende do fornecedor do switch e do suporte do sistema de armazenamento para configurações FCoE.

A contagem de saltos é definida como o número de switches no caminho entre o iniciador (host) e o destino (sistema de armazenamento). A documentação da Cisco Systems também se refere a esse valor como o *diâmetro da malha SAN*.

Para FCoE, você pode ter switches FCoE conetados a switches FC.

Para conexões FCoE de ponta a ponta, os switches FCoE devem estar executando uma versão de firmware que suporte ISLs (links inter-switch Ethernet).

A tabela a seguir lista o máximo de contagens de saltos suportadas:

Fornecedor do interrutor	Contagem de saltos suportada
Brocade	7 para FC 5 para FCoE
Cisco	7 Até 3 dos switches podem ser switches FCoE.

Zoneamento Fibre Channel e FCoE

Visão geral do zoneamento Fibre Channel e FCoE

Uma zona FC, FC-NVMe ou FCoE é um agrupamento lógico de uma ou mais portas em uma malha. Para que os dispositivos possam se ver, conetar, criar sessões entre si e se comunicar, ambas as portas precisam ter uma associação de zona comum. Recomenda-se um zoneamento de iniciador único.

Razões para o zoneamento

- O zoneamento reduz ou elimina *crosstalk* entre HBAs iniciador.

  Isso ocorre mesmo em ambientes pequenos e é um dos melhores argumentos para a implementação do zoneamento. Os subconjuntos de tecido lógico criados pelo zoneamento eliminam problemas de conversa cruzada.

- O zoneamento reduz o número de caminhos disponíveis para uma porta FC, FC-NVMe ou FCoE específica e reduz o número de caminhos entre um host e um LUN específico visível.

  Por exemplo, algumas soluções de multipathing do sistema operacional host têm um limite no número de caminhos que podem gerenciar. O zoneamento pode reduzir o número de caminhos que um driver de multipathing do sistema operacional vê. Se um host não tiver uma solução multipathing instalada, você precisará verificar se apenas um caminho para um LUN é visível usando o zoneamento na malha ou uma combinação de mapeamento de LUN seletivo (SLM) e portsets no SVM.

- O zoneamento aumenta a segurança limitando o acesso e a conetividade a pontos finais que compartilham uma zona comum.

  Portas que não têm zonas em comum não podem se comunicar umas com as outras.

- O zoneamento melhora a confiabilidade da SAN isolando problemas que ocorrem e ajuda a reduzir o tempo de resolução de problemas limitando o espaço do problema.

Recomendações para zoneamento

- Você deve implementar o zoneamento a qualquer momento, se quatro ou mais hosts estiverem conetados a uma SAN ou se o SLM não for implementado nos nós a uma SAN.
- Embora o World Wide Node Name zoning seja possível com alguns fornecedores de switch, o World Wide Port Name zoning é necessário para definir adequadamente uma porta específica e usar o NPIV de forma eficaz.
- Você deve limitar o tamanho da zona, mantendo a capacidade de gerenciamento.

  Várias zonas podem se sobrepor ao tamanho limite. Idealmente, uma zona é definida para cada host ou cluster de host.

- Você deve usar o zoneamento de um único iniciador para eliminar a interferência cruzada entre HBAs do iniciador.

Zoneamento baseado em nome mundial

O zoneamento baseado no World Wide Name (WWN) especifica o WWN dos membros a serem incluídos na zona. Ao zonear no ONTAP, você deve usar o zoneamento de nome de porta mundial (WWPN).

WWPN zoneamento fornece flexibilidade porque o acesso não é determinado por onde o dispositivo está fisicamente conetado à malha. Você pode mover um cabo de uma porta para outra sem reconfigurar zonas.

Para caminhos Fibre Channel para controladores de storage que executam ONTAP, verifique se os switches FC estão zoneados usando WWPNs das interfaces lógicas de destino (LIFs), e não as WWPNs das portas físicas no nó. Para obter mais informações sobre LIFs, consulte o *Guia de Gerenciamento de rede do ONTAP*.

"Gerenciamento de rede"

Zonas individuais

Na configuração de zoneamento recomendada, há um iniciador de host por zona. A zona consiste na porta do iniciador do host e em um ou mais LIFs de destino nos nós de storage que estão fornecendo acesso aos LUNs até o número desejado de caminhos por destino. Isso significa que os hosts que acessam os mesmos nós não podem ver as portas uns dos outros, mas cada iniciador pode acessar qualquer nó.

Você deve adicionar todos os LIF da máquina virtual de armazenamento (SVM) na zona com o iniciador do host. Isso permite que você mova volumes ou LUNs sem editar suas zonas existentes ou criar novas zonas.

Para caminhos de Fibre Channel para nós que executam ONTAP, certifique-se de que os switches FC sejam zoneados usando WWPNs das interfaces lógicas de destino (LIFs), e não as WWPNs das portas físicas no nó. As WWPNs dos portos físicos começam com "50" e as WWPNs dos LIFs começam com ""20"".

Zoneamento de tecido único

Em uma configuração de estrutura única, você ainda pode conectar cada iniciador de host a cada nó de storage. O software multipathing é necessário no host para gerenciar vários caminhos. Cada host deve ter dois iniciadores para multipathing para fornecer resiliência na solução.

Cada iniciador deve ter um mínimo de um LIF de cada nó que o iniciador possa acessar. O zoneamento deve permitir pelo menos um caminho do iniciador do host para o par de nós de HA no cluster para fornecer um caminho para a conetividade LUN. Isso significa que cada iniciador no host pode ter apenas um LIF de destino por nó em sua configuração de zona. Se houver um requisito de multipathing para o mesmo nó ou vários nós no cluster, cada nó terá várias LIFs por nó em sua configuração de zona. Isso permite que o host ainda acesse seus LUNs se um nó falhar ou se um volume contendo o LUN for movido para um nó diferente. Isso também requer que os nós de relatório sejam definidos adequadamente.

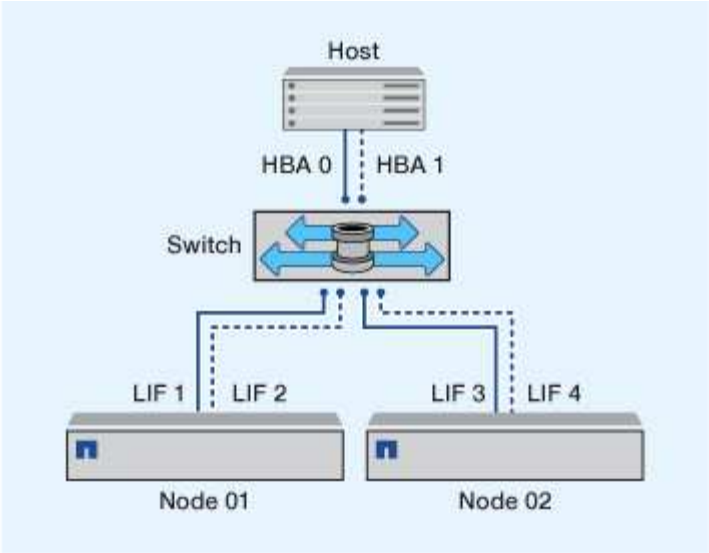
Configurações de estrutura única são compatíveis, mas não são consideradas altamente disponíveis. A falha de um único componente pode causar perda de acesso aos dados.

Na figura a seguir, o host tem dois iniciadores e está executando software multipathing. Existem duas zonas:

> A convenção de nomenclatura usada nesta figura é apenas uma recomendação de uma possível convenção de nomenclatura que você pode escolher usar para sua solução ONTAP.

- Zona 1: HBA 0, LIF_1 e LIF_3
- Zona 2: HBA 1, LIF_2 e LIF_4

Se a configuração incluísse mais nós, as LIFs para os nós adicionais seriam incluídas nessas zonas.



Neste exemplo, você também pode ter todos os quatro LIFs em cada zona. Nesse caso, as zonas seriam as seguintes:

- Zona 1: HBA 0, LIF_1, LIF_2, LIF_3 e LIF_4
- Zona 2: HBA 1, LIF_1, LIF_2, LIF_3 e LIF_4

O sistema operacional host e o software de multipathing precisam dar suporte ao número de caminhos compatíveis que estão sendo usados para acessar os LUNs nos nós. Para determinar o número de caminhos usados para acessar os LUNs nos nós, consulte a seção limites de configuração da SAN.

Informações relacionadas

"NetApp Hardware Universe"

Zoneamento de par HA de estrutura dupla

Em configurações de estrutura dupla, é possível conectar cada iniciador de host a cada nó de cluster. Cada iniciador de host usa um switch diferente para acessar os nós de cluster. O software multipathing é necessário no host para gerenciar vários caminhos.

Configurações de estrutura dupla são consideradas de alta disponibilidade porque o acesso aos dados é mantido em caso de falha em um único componente.

Na figura a seguir, o host tem dois iniciadores e está executando software multipathing. Existem duas zonas. O SLM é configurado para que todos os nós sejam considerados como nós de relatório.

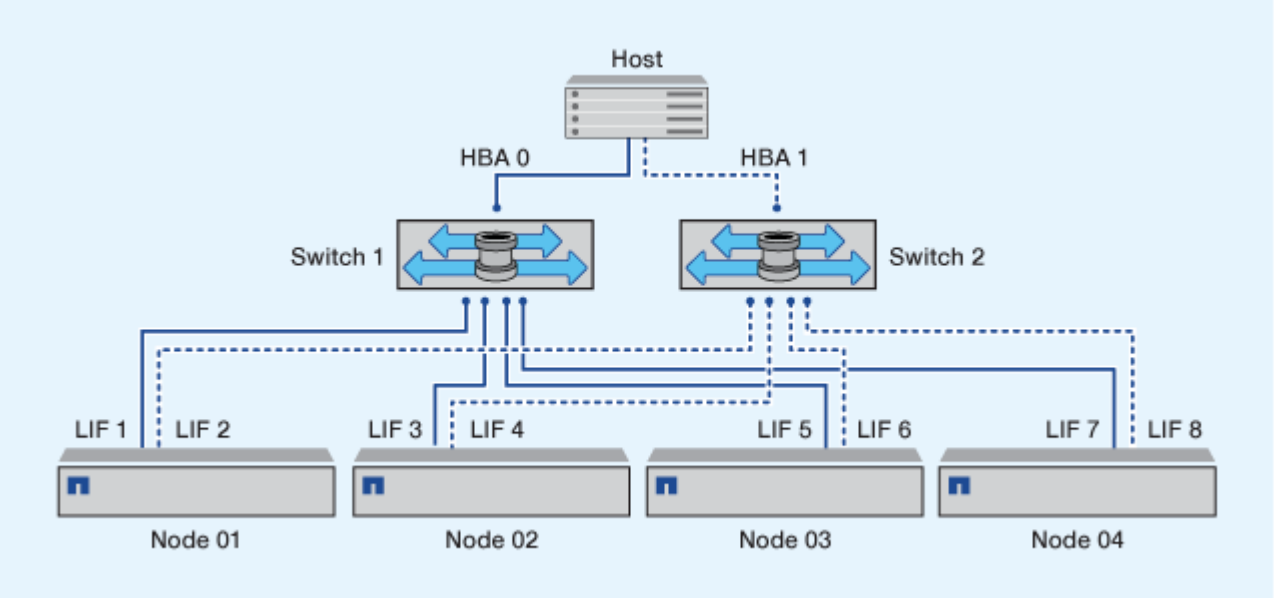
A convenção de nomenclatura usada nesta figura é apenas uma recomendação de uma possível convenção de nomenclatura que você pode escolher usar para sua solução ONTAP.

- Zona 1: HBA 0, LIF_1, LIF_3, LIF_5 e LIF_7
- Zona 2: HBA 1, LIF_2, LIF_4, LIF_6 e LIF_8

Cada iniciador do host é zoneado por um switch diferente. A zona 1 é acessada através do interrutor 1. A zona 2 é acessada através do interrutor 2.

Cada iniciador pode acessar um LIF em cada nó. Isso permite que o host ainda acesse LUNs se um nó falhar. Os SVMs têm acesso a todas as LIFs iSCSI e FC em cada nó em uma solução em cluster com base na configuração de mapa LUN seletivo (SLM) e na configuração do nó de relatório. Você pode usar o zoneamento de switch SLM, portsets ou FC para reduzir o número de caminhos de uma SVM para o host e o número de caminhos de uma SVM para um LUN.

Se a configuração incluísse mais nós, as LIFs para os nós adicionais seriam incluídas nessas zonas.



O sistema operacional host e o software multipathing precisam dar suporte ao número de caminhos que estão sendo usados para acessar os LUNs nos nós.

Informações relacionadas

"NetApp Hardware Universe"

Restrições de zoneamento para switches Cisco FC e FCoE

Ao usar os switches FC e FCoE Cisco, uma única zona de malha não deve conter mais de um LIF de destino para a mesma porta física. Se várias LIFs na mesma porta estiverem na mesma zona, as portas LIF podem falhar ao recuperar de uma perda de conexão.

Os switches FC comuns são usados no protocolo FC-NVMe da mesma maneira que são usados no protocolo FC.

- Várias LIFs para os protocolos FC e FCoE podem compartilhar portas físicas em um nó, contanto que estejam em zonas diferentes.
- O FC-NVMe e o FCoE não podem compartilhar a mesma porta física.
- FC e FC-NVMe podem compartilhar a mesma porta física de 32 GB.
- Os switches FC e FCoE da Cisco exigem que cada LIF em uma determinada porta esteja em uma zona separada das outras LIFs nessa porta.
- Uma única zona pode ter LIFs FC e FCoE. Uma zona pode conter um LIF de cada porta de destino no cluster, mas tenha cuidado para não exceder os limites de caminho do host e verificar a configuração do SLM.

- LIFs em diferentes portas físicas podem estar na mesma zona.
- Os switches Cisco exigem que os LIFs sejam separados.

  Embora não seja necessário, recomenda-se separar LIFs para todos os switches

Requisitos para configurações de SAN compartilhadas

Configurações de SAN compartilhadas são definidas como hosts conectados aos sistemas de storage da ONTAP e aos sistemas de storage de outros fornecedores. O acesso aos sistemas de storage da ONTAP e aos sistemas de storage de outros fornecedores a partir de um único host é suportado, desde que sejam atendidos vários requisitos.

Para todos os sistemas operacionais host, é uma prática recomendada usar adaptadores separados para se conetar aos sistemas de storage de cada fornecedor. O uso de adaptadores separados reduz as chances de drivers e configurações conflitantes. Para conexões com um sistema de armazenamento ONTAP, o modelo do adaptador, BIOS, firmware e driver devem ser listados como suportados na ferramenta de Matriz de interoperabilidade do NetApp.

Você deve definir os valores de tempo limite necessários ou recomendados e outros parâmetros de armazenamento para o host. Você deve sempre instalar o software NetApp ou aplicar as configurações do NetApp por último.

- Para o AIX, você deve aplicar os valores da versão do AIX Host Utilities listada na ferramenta de Matriz de interoperabilidade para sua configuração.
- Para o ESX, você deve aplicar as configurações do host usando o Virtual Storage Console para VMware vSphere.
- Para HP-UX, você deve usar as configurações de armazenamento padrão HP-UX.
- Para Linux, você deve aplicar os valores da versão Linux Host Utilities listada na ferramenta de Matriz de interoperabilidade para sua configuração.
- Para o Solaris, você deve aplicar os valores da versão do Solaris Host Utilities listada na ferramenta de Matriz de interoperabilidade para sua configuração.
- Para o Windows, você deve instalar a versão do Windows Host Utilities que está listada na ferramenta de Matriz de interoperabilidade para sua configuração.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

Configurações DE SAN em um ambiente MetroCluster

Configurações DE SAN em um ambiente MetroCluster

Você precisa estar ciente de algumas considerações ao usar configurações de SAN em um ambiente MetroCluster.

- As configurações do MetroCluster não são compatíveis com configurações VSAN "roteadas" de malha FC de front-end.
- A partir do ONTAP 9.15,1, as configurações de IP MetroCluster de quatro nós são compatíveis com NVMe/TCP.

- A partir do ONTAP 9.12,1, as configurações de IP MetroCluster de quatro nós são compatíveis com NVMe/FC. As configurações do MetroCluster não são compatíveis com redes NVMe front-end anteriores ao ONTAP 9.12,1.
- Outros protocolos SAN, como iSCSI, FC e FCoE, são compatíveis com configurações do MetroCluster.
- Ao usar configurações de cliente SAN, você deve verificar se quaisquer considerações especiais para configurações do MetroCluster estão incluídas nas notas fornecidas no "Ferramenta de Matriz de interoperabilidade do NetApp" (IMT).
- Os sistemas operacionais e os aplicativos devem fornecer resiliência de e/S de 120 segundos para dar suporte ao switchover não planejado automático da MetroCluster e ao switchover tiebreaker ou iniciado por Mediator.
- As configurações do MetroCluster usam as mesmas WWNNs e WWPNs em ambos os lados da malha FC de front-end.

Informações relacionadas

- "Compreender a proteção de dados e a recuperação de desastres da MetroCluster"
- "artigo da Knowledge base: Quais são as considerações de suporte ao host AIX em uma configuração do MetroCluster?"
- "artigo da base de conhecimento: Considerações de suporte a hosts Solaris em uma configuração do MetroCluster"

Evite a sobreposição de portas entre switchover e switchback

Em um ambiente SAN, você pode configurar os switches front-end para evitar sobreposição quando a porta antiga fica off-line e a nova porta entra on-line.

Durante o switchover, a porta FC no local sobrevivente pode fazer login na malha antes que a malha detete que a porta FC no local de desastre está off-line e removeu essa porta dos serviços de nome e diretório.

Se a porta FC no desastre ainda não for removida, a tentativa de login da malha da porta FC no local sobrevivente pode ser rejeitada devido a uma WWPN duplicada. Esse comportamento dos switches FC pode ser alterado para honrar o login do dispositivo anterior e não o existente. Você deve verificar os efeitos desse comportamento em outros dispositivos de malha. Entre em Contato com o fornecedor do switch para obter mais informações.

Escolha o procedimento correto de acordo com o seu tipo de interrutor.

Exemplo 9. Passos

Interrutor Cisco

1. Ligue ao interrutor e inicie sessão.
2. Entre no modo de configuração:

```
switch# config t
switch(config)#
```

3. Substituir a primeira entrada de dispositivo na base de dados do servidor de nomes pelo novo dispositivo:

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. Nos switches que estão executando o NX-os 8.x, confirme se o tempo limite do flogi quiesce está definido como zero:

   a. Apresentar o timererval quiesce:

   ```
   switch(config)# show flogi interval info \| i quiesce
   ```

   ```
   Stats:  fs flogi quiesce timerval:  0
   ```

   b. Se a saída na etapa anterior não indicar que o timerval é zero, defina-o como zero:

   ```
   switch(config)# flogi scale enable
   ```

```
switch(config)$ flogi quiesce timeout 0
```

Interrutor Brocade

1. Ligue ao interrutor e inicie sessão.
2. Introduza o `switchDisable` comando.
3. Digite o `configure` comando e pressione `y` no prompt.

```
F-Port login parameters (yes, y, no, n): [no] y
```

4. Escolha a definição 1:

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. Responda aos prompts restantes, ou pressione **Ctrl D**.
6. Introduza o `switchEnable` comando.

Informações relacionadas

"Realização de comutação para testes ou manutenção"

Suporte de host para multipathing

Suporte de host para visão geral de multipathing

O ONTAP sempre usa o Acesso lógico de Unidade assimétrica (ALUA) para caminhos FC e iSCSI. Use configurações de host compatíveis com ALUA para protocolos FC e iSCSI.

A partir do par de HA multipath ONTAP 9.5, o failover/giveback é compatível com configurações NVMe usando o acesso de namespace assíncrono (ANA). No ONTAP 9.4, o NVMe só oferece suporte a um caminho do host para o destino. O host de aplicações precisa gerenciar o failover de caminho para seu parceiro de alta disponibilidade (HA).

Para obter informações sobre quais configurações de host específicas suportam ALUA ou ANA, consulte "Ferramenta de Matriz de interoperabilidade do NetApp" e "Configuração do host SAN ONTAP" para o sistema operacional do seu host.

Quando o software de multipathing do host é necessário

Se houver mais de um caminho das interfaces lógicas (LIFs) da máquina virtual de storage (SVM) para a malha, é necessário software de multipathing. O software multipathing é necessário no host sempre que o host puder acessar um LUN por mais de um caminho.

O software multipathing apresenta um único disco para o sistema operacional para todos os caminhos para um LUN. Sem software multipathing, o sistema operacional poderia tratar cada caminho como um disco separado, o que pode levar à corrupção de dados.

Sua solução é considerada como tendo vários caminhos se você tiver qualquer um dos seguintes:

- Uma única porta de iniciador no host que é anexada a várias LIFs SAN no SVM
- Várias portas de iniciador anexando a um único LIF de SAN no SVM
- Várias portas de iniciador anexadas a várias LIFs SAN no SVM

O software multipathing é recomendado em configurações de HA. Além do mapa LUN seletivo, é recomendável usar o zoneamento de switch FC ou portsets para limitar os caminhos usados para acessar LUNs.

O software multipathing também é conhecido como software MPIO (multipath I/o).

Número recomendado de caminhos do host para nós no cluster

Você não deve exceder mais de oito caminhos do host para cada nó do cluster, prestando atenção ao número total de caminhos que podem ser suportados pelo sistema

operacional do host e pelo multipathing usado no host.

Você deve ter no mínimo dois caminhos por LUN conetando-se a cada nó de relatório por meio do mapa de LUN seletivo (SLM) usado pela máquina virtual de storage (SVM) no cluster. Isso elimina pontos únicos de falha e permite que o sistema sobreviva a falhas de componentes.

Se você tiver quatro ou mais nós no cluster ou mais de quatro portas de destino sendo usadas pelas SVMs em qualquer um de seus nós, use os métodos a seguir para limitar o número de caminhos que podem ser usados para acessar LUNs em seus nós, de modo que você não exceda o máximo recomendado de oito caminhos.

- SLM

  O SLM reduz o número de caminhos do host para o LUN para apenas caminhos no nó proprietário do LUN e do parceiro de HA do nó proprietário. O SLM está ativado por predefinição.

- Portsets para iSCSI
- Mapeamentos do grupo FC de seu host
- Zoneamento do switch FC

Informações relacionadas

"Administração da SAN"

Limites de configuração

Determine o número de nós suportados para configurações SAN

O número de nós por cluster com suporte do ONTAP varia de acordo com a versão do ONTAP, os modelos de controlador de storage no cluster e o protocolo dos nós do cluster.

Sobre esta tarefa

Se qualquer nó no cluster estiver configurado para FC, FC-NVMe, FCoE ou iSCSI, esse cluster estará limitado aos limites de nó SAN. Os limites de nó baseados nos controladores do cluster são listados em *Hardware Universe*.

Passos

1. Vá para "NetApp Hardware Universe".
2. Clique em **plataformas** no canto superior esquerdo (ao lado do botão **Home**) e selecione o tipo de plataforma.
3. Marque a caixa de seleção ao lado de sua versão do ONTAP.

   Uma nova coluna é exibida para você escolher suas plataformas.

4. Marque as caixas de seleção ao lado das plataformas usadas em sua solução.
5. Desmarque a caixa de seleção **Selecionar tudo** na coluna **escolha suas especificações**.
6. Marque a caixa de seleção **máximo de nós por cluster (nas/SAN)**.
7. Clique em **Mostrar resultados**.

Informações relacionadas

"NetApp Hardware Universe"

Determine o número de hosts com suporte por cluster nas configurações FC e FC-NVMe

O número máximo de hosts SAN que podem ser conetados a um cluster varia muito com base em sua combinação específica de vários atributos de cluster, como o número de hosts conetados a cada nó de cluster, iniciadores por host, sessões por host e nós no cluster.

Sobre esta tarefa

Para configurações FC e FC-NVMe, use o número de nexos de iniciador-destino (ITNs) no sistema para determinar se é possível adicionar mais hosts ao cluster.

Uma ITN representa um caminho desde o iniciador do host até o destino do sistema de armazenamento. O número máximo de ITNs por nó nas configurações FC e FC-NVMe é de 2.048. Contanto que você esteja abaixo do número máximo de ITNs, você pode continuar adicionando hosts ao cluster.

Para determinar o número de ITNs usados no cluster, execute as etapas a seguir para cada nó no cluster.

Passos

1. Identifique todas as LIFs em um determinado nó.
2. Execute o seguinte comando para cada LIF no nó:

   ```
   fcp initiator show -fields wwpn, lif
   ```

   O número de entradas exibidas na parte inferior da saída do comando representa o número de ITNs para esse LIF.

3. Registre o número de ITNs exibidos para cada LIF.
4. Adicione o número de ITNs para cada LIF em cada nó do cluster.

   Esse total representa o número de ITNs em seu cluster.

Determine o número suportado de hosts em configurações iSCSI

O número máximo de hosts SAN que podem ser conetados em configurações iSCSI varia muito com base em sua combinação específica de vários atributos de cluster, como o número de hosts conetados a cada nó de cluster, iniciadores por host, logins por host e nós no cluster.

Sobre esta tarefa

O número de hosts que podem ser conetados diretamente a um nó ou que podem ser conetados por meio de um ou mais switches depende do número de portas Ethernet disponíveis. O número de portas Ethernet disponíveis é determinado pelo modelo do controlador e pelo número e tipo de adaptadores instalados no controlador. O número de portas Ethernet suportadas para controladores e adaptadores está disponível em *Hardware Universe*.

Para todas as configurações de cluster de vários nós, você deve determinar o número de sessões iSCSI por nó para saber se você pode adicionar mais hosts ao cluster. Desde que o cluster esteja abaixo do número máximo de sessões iSCSI por nó, você pode continuar a adicionar hosts ao cluster. O número máximo de sessões iSCSI por nó varia de acordo com os tipos de controladores no cluster.

Passos

1. Identifique todos os grupos de portal de destino no nó.
2. Verifique o número de sessões iSCSI para cada grupo de portal de destino no nó:

   `iscsi session show -tpgroup` *`tpgroup`*

   O número de entradas exibidas na parte inferior da saída do comando representa o número de sessões iSCSI para esse grupo de portal de destino.

3. Registe o número de sessões iSCSI apresentadas para cada grupo de portal de destino.
4. Adicione o número de sessões iSCSI para cada grupo de portal de destino no nó.

   O total representa o número de sessões iSCSI no nó.

Limites de configuração do switch FC

Os switches Fibre Channel têm limites máximos de configuração, incluindo o número de logins suportados por porta, grupo de portas, blade e switch. Os fornecedores de switch documentam seus limites suportados.

Cada interface lógica FC (LIF) faz logon em uma porta de switch FC. O número total de logins de um único destino no nó é igual ao número de LIFs mais um login para a porta física subjacente. Não exceda os limites de configuração do fornecedor do switch para logins ou outros valores de configuração. Isso também é válido para os iniciadores que estão sendo usados no lado do host em ambientes virtualizados com NPIV habilitado. Não exceda os limites de configuração do fornecedor do switch para logins para o destino ou os iniciadores que estão sendo usados na solução.

Limites do interrutor Brocade

Você pode encontrar os limites de configuração para switches Brocade nas *Diretrizes de escalabilidade Brocade*.

Limites do switch dos sistemas Cisco

Você pode encontrar os limites de configuração para switches Cisco "Limites de configuração do Cisco" no guia para sua versão do software de switch Cisco.

Calcular a visão geral da profundidade da fila

Talvez seja necessário ajustar a profundidade da fila FC no host para alcançar os valores máximos de ITNs por nó e ventilador de porta FC. O número máximo de LUNs e o número de HBAs que podem se conetar a uma porta FC são limitados pela profundidade de fila disponível nas portas de destino FC.

Sobre esta tarefa

A profundidade da fila é o número de solicitações de e/S (comandos SCSI) que podem ser enfileiradas em uma controladora de armazenamento. Cada solicitação de e/S do HBA iniciador do host para o adaptador de destino do controlador de armazenamento consome uma entrada de fila. Normalmente, uma maior profundidade de fila equivale a um melhor desempenho. No entanto, se a profundidade máxima da fila do controlador de armazenamento for atingida, esse controlador de armazenamento rejeita os comandos de entrada retornando uma resposta QFULL a eles. Se um grande número de hosts estiver acessando um

controlador de armazenamento, você deve Planejar cuidadosamente para evitar condições QFULL, que degradam significativamente o desempenho do sistema e podem levar a erros em alguns sistemas.

Em uma configuração com vários iniciadores (hosts), todos os hosts devem ter profundidades de fila semelhantes. Devido à desigualdade na profundidade da fila entre os hosts conetados ao controlador de armazenamento através da mesma porta de destino, os hosts com menores profundidades de fila estão sendo privados de acesso a recursos por hosts com maiores profundidades de fila.

As seguintes recomendações gerais podem ser feitas sobre as profundidades da fila "sintonização":

- Para sistemas de tamanho pequeno a médio, utilize uma profundidade de fila HBA de 32 mm.
- Para sistemas grandes, utilize uma profundidade de fila HBA de 128 mm.
- Para casos de exceção ou teste de desempenho, use uma profundidade de fila de 256 mm para evitar possíveis problemas de enfileiramento.
- Todos os hosts devem ter as profundidades da fila definidas para valores semelhantes para dar acesso igual a todos os hosts.
- Para evitar penalidades ou erros de desempenho, a profundidade da fila da porta FC de destino do controlador de storage não deve ser excedida.

Passos

1. Conte o número total de iniciadores FC em todos os hosts que se conetam a uma porta de destino FC.
2. Multiplique por 128.
   - Se o resultado for inferior a 2.048, defina a profundidade da fila para todos os iniciadores como 128. Você tem 15 hosts com um iniciador conetado a cada uma das duas portas de destino no controlador de storage. 15 x 128: 1.920. Como 1.920 é menor do que o limite total de profundidade de fila de 2.048, você pode definir a profundidade de fila para todos os iniciadores como 128.
   - Se o resultado for superior a 2.048, avance para o passo 3. Você tem 30 hosts com um iniciador conetado a cada uma das duas portas de destino no controlador de storage. 30 x 128: 3.840. Como o 3.840 é maior do que o limite total de profundidade de fila de 2.048, você deve escolher uma das opções na etapa 3 para correção.
3. Escolha uma das opções a seguir para adicionar mais hosts ao controlador de storage.
   - Opção 1:
     i. Adicione mais portas de destino FC.
     ii. Redistribua seus iniciadores FC.
     iii. Repita os passos 1 e 2. A profundidade de fila desejada de 3.840 mm excede a profundidade de fila disponível por porta. Para remediar isso, você pode adicionar um adaptador de destino FC de duas portas a cada controlador e, em seguida, rezonear seus switches FC para que 15 dos seus hosts 30 se conetem a um conjunto de portas e os 15 hosts restantes se conetem a um segundo conjunto de portas. A profundidade da fila por porta é então reduzida para 15 x 128, ou seja, 1.920.
   - Opção 2:
     i. Designe cada host como "grande" ou "shopping" com base em sua necessidade de e/S esperada.
     ii. Multiplique o número de grandes iniciadores por 128.
     iii. Multiplique o número de pequenos iniciadores por 32.
     iv. Adicione os dois resultados juntos.
     v. Se o resultado for inferior a 2.048, defina a profundidade da fila para hosts grandes para 128 e a

profundidade da fila para hosts pequenos para 32.

vi. Se o resultado ainda for superior a 2.048 por porta, reduza a profundidade da fila por iniciador até que a profundidade total da fila seja inferior ou igual a 2.048.

> Para estimar a profundidade da fila necessária para obter uma determinada taxa de transferência de e/S por segundo, use esta fórmula:
>
> Profundidade da fila necessária (número de e/S por segundo) x (tempo de resposta)
>
> Por exemplo, se você precisar de 40.000 I/o por segundo com um tempo de resposta de 3 milissegundos, a profundidade de fila necessária é de 40.000 x (.003), ou seja, 120.

O número máximo de hosts que você pode se conetar a uma porta de destino é 64, se você decidir limitar a profundidade da fila à recomendação básica de 32. No entanto, se você decidir ter uma profundidade de fila de 128, então você pode ter um máximo de 16 hosts conetados a uma porta de destino. Quanto maior a profundidade da fila, menos hosts que uma única porta de destino pode suportar. Se sua exigência for tal que você não pode comprometer a profundidade da fila, então você deve obter mais portas de destino.

A profundidade de fila pretendida de 3.840 mm excede a profundidade de fila disponível por porta. Você tem 10 hosts grandes que têm altas necessidades de e/S de armazenamento e 20 hosts "shopping" que têm baixas necessidades de e/S. Defina a profundidade da fila do iniciador nos hosts grandes para 128 e a profundidade da fila do iniciador nos hosts pequenos para 32.

A profundidade total da fila resultante é de (10 x 128) (20 x 32) 1.920.

Você pode espalhar a profundidade da fila disponível igualmente em cada iniciador.

A profundidade da fila resultante por iniciador é de 2.048 ÷ 30 68.

Defina as profundidades da fila em hosts SAN

Talvez seja necessário alterar as profundidades da fila em seu host para alcançar os valores máximos de ITNs por nó e ventilador de porta FC.

AIX anfitriões

Você pode alterar a profundidade da fila em hosts AIX usando o `chdev` comando. As alterações feitas usando o `chdev` comando persistem nas reinicializações.

Exemplos:

- Para alterar a profundidade da fila do dispositivo hdisk7, use o seguinte comando:

  ```
  chdev -l hdisk7 -a queue_depth=32
  ```

- Para alterar a profundidade da fila para o HBA fcs0, use o seguinte comando:

  ```
  chdev -l fcs0 -a num_cmd_elems=128
  ```

  O valor padrão para `num_cmd_elems` é 200. O valor máximo é 2.048.

Pode ser necessário colocar o HBA off-line para mudar `num_cmd_elems` e depois colocá-lo de volta on-line usando os `rmdev -l fcs0 -R` comandos e. `makdev -l fcs0 -P`

Hosts HP-UX

Você pode alterar a profundidade da fila de LUN ou dispositivo em hosts HP-UX usando o parâmetro kernel `scsi_max_qdepth` . Você pode alterar a profundidade da fila HBA usando o parâmetro kernel `max_fcp_reqs` .

- O valor padrão para `scsi_max_qdepth` é 8. O valor máximo é 255.

  `scsi_max_qdepth` pode ser alterado dinamicamente em um sistema em execução usando a `-u` opção no `kmtune` comando. A alteração será efetiva para todos os dispositivos no sistema. Por exemplo, use o seguinte comando para aumentar a profundidade da fila de LUN para 64:

  ```
  kmtune -u -s scsi_max_qdepth=64
  ```

  É possível alterar a profundidade da fila para arquivos de dispositivos individuais usando o `scsictl` comando. As alterações usando o `scsictl` comando não são persistentes em todas as reinicializações do sistema. Para exibir e alterar a profundidade da fila de um arquivo de dispositivo específico, execute o seguinte comando:

  ```
  scsictl -a /dev/rdsk/c2t2d0

  scsictl -m queue_depth=16 /dev/rdsk/c2t2d0
  ```

- O valor padrão para `max_fcp_reqs` é 512. O valor máximo é 1024.

  O kernel deve ser reconstruído e o sistema deve ser reinicializado para que as alterações `max_fcp_reqs` entrem em vigor. Para alterar a profundidade da fila HBA para 256, por exemplo, use o seguinte comando:

  ```
  kmtune -u -s max_fcp_reqs=256
  ```

Hosts Solaris

Você pode definir a profundidade da fila de LUN e HBA para seus hosts Solaris.

- Para a profundidade da fila de LUN: O número de LUNs em uso em um host multiplicado pelo acelerador por lun (profundidade da fila de lun) deve ser menor ou igual ao valor de profundidade da fila de tgt no host.
- Para a profundidade da fila em uma pilha Sun: Os drivers nativos não permitem configurações por LUN ou por destino `max_throttle` no nível HBA. O método recomendado para definir o `max_throttle` valor para drivers nativos está em um nível por tipo de dispositivo (VID_PID) nos `/kernel/drv/sd.conf` arquivos e `/kernel/drv/ssd.conf`. O utilitário de host define esse valor como 64 para configurações MPxIO e 8 para configurações Veritas DMP.

Passos

1. `# cd/kernel/drv`
2. `# vi lpfc.conf`
3. PESQUISE `/tft-queue (/tgt-queue)`

```
tgt-queue-depth=32
```

O valor padrão é definido como 32 na instalação.

4. Defina o valor desejado com base na configuração do seu ambiente.
5. Salve o arquivo.
6. Reinicie o host usando o `sync; sync; sync; reboot -- -r` comando.

Hosts VMware para um HBA QLogic

Use o `esxcfg-module` comando para alterar as configurações de tempo limite do HBA. A atualização manual do `esx.conf` ficheiro não é recomendada.

Passos

1. Faça logon no console de serviço como usuário raiz.
2. Use o `#vmkload_mod -l` comando para verificar qual módulo Qlogic HBA está atualmente carregado.
3. Para uma única instância de um Qlogic HBA, execute o seguinte comando:

```
#esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
```

Este exemplo usa o módulo qla2300_707. Use o módulo apropriado com base na saída do `vmkload_mod -l`.

4. Salve suas alterações usando o seguinte comando:

```
#/usr/sbin/esxcfg-boot -b
```

5. Reinicie o servidor usando o seguinte comando:

```
#reboot
```

6. Confirme as alterações utilizando os seguintes comandos:
   a. `#esxcfg-module -g qla2300_707`
   b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

Hosts VMware para um Emulex HBA

Use o `esxcfg-module` comando para alterar as configurações de tempo limite do HBA. A atualização manual do `esx.conf` ficheiro não é recomendada.

Passos

1. Faça logon no console de serviço como usuário raiz.
2. Use o `#vmkload_mod -l grep lpfc` comando para verificar qual Emulex HBA está atualmente carregado.
3. Para uma única instância de um Emulex HBA, digite o seguinte comando:

```
#esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```

Dependendo do modelo do HBA, o módulo pode ser lpfcdd_7xx ou lpfcdd_732. O comando acima usa o módulo lpfcdd_7xx. Você deve usar o módulo apropriado com base no resultado `vmkload_mod -l` do .

Executar este comando irá definir a profundidade da fila de LUN para 16 para o HBA representado por lpfc0.

4. Para várias instâncias de um Emulex HBA, execute o seguinte comando:

```
a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
lpfcdd_7xx
```

A profundidade da fila LUN para lpfc0 e a profundidade da fila LUN para lpfc1 estão definidas para 16.

5. Introduza o seguinte comando:

```
#esxcfg-boot -b
```

6. Reinicie usando `#reboot`o .

Windows hosts para um Emulex HBA

Em hosts do Windows, você pode usar o `LPUTILNT` utilitário para atualizar a profundidade da fila para HBAs Emulex.

Passos

1. Execute o `LPUTILNT` utilitário localizado no `C:\WINNT\system32` diretório.
2. Selecione **Drive Parameters** no menu à direita.
3. Role para baixo e clique duas vezes em **QueueDepth**.

Se você estiver definindo **QueueDepth** maior que 150, o seguinte valor do Registro do Windows também precisará ser aumentado adequadamente:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests
```

Hosts do Windows para um HBA Qlogic

Em hosts do Windows, você pode usar o `SANsurfer` utilitário gerenciador HBA para atualizar as profundidades da fila para HBAs Qlogic.

Passos

1. Execute o `SANsurfer` utilitário gerenciador HBA.
2. Clique em **HBA port** > **Settings**.
3. Clique em **Advanced HBA port settings** (Definições avançadas da porta HBA) na caixa de listagem.
4. Atualize `Execution Throttle` o parâmetro.

Hosts Linux para Emulex HBA

Você pode atualizar as profundidades da fila de um Emulex HBA em um host Linux. Para tornar as atualizações persistentes nas reinicializações, você deve criar uma nova imagem de disco RAM e reinicializar o host.

Passos

1. Identificar os parâmetros de profundidade da fila a modificar:

   ```
   modinfo lpfc|grep queue_depth
   ```

   É apresentada a lista de parâmetros de profundidade da fila com a respetiva descrição. Dependendo da versão do sistema operacional, você pode modificar um ou mais dos seguintes parâmetros de profundidade de fila:

   - `lpfc_lun_queue_depth`: Número máximo de comandos FC que podem ser enfileirados para um LUN específico (uint)
   - `lpfc_hba_queue_depth`: Número máximo de comandos FC que podem ser enfileirados para um HBA lpfc (uint)
   - `lpfc_tgt_queue_depth`: Número máximo de comandos FC que podem ser enfileirados para uma porta de destino específica (uint)

     O `lpfc_tgt_queue_depth` parâmetro é aplicável somente para sistemas Red Hat Enterprise Linux 7.x, sistemas SUSE Linux Enterprise Server 11 SP4 e sistemas 12.x.

2. Atualize as profundidades da fila adicionando os parâmetros de profundidade da fila ao `/etc/modprobe.conf` arquivo de um sistema Red Hat Enterprise Linux 5.x e ao `/etc/modprobe.d/scsi.conf` arquivo de um sistema Red Hat Enterprise Linux 6.x ou 7.x, ou de um sistema SUSE Linux Enterprise Server 11.x ou 12.x.

   Dependendo da versão do sistema operacional, você pode adicionar um ou mais dos seguintes comandos:

   - `options lpfc lpfc_hba_queue_depth=new_queue_depth`
   - `options lpfc lpfc_lun_queue_depth=new_queue_depth`
   - `options lpfc_tgt_queue_depth=new_queue_depth`

3. Crie uma nova imagem de disco RAM e reinicie o host para tornar as atualizações persistentes nas reinicializações.

   Para obter mais informações, consulte o "Administração do sistema" para sua versão do sistema operacional Linux.

4. Verifique se os valores de profundidade da fila são atualizados para cada parâmetro de profundidade da fila que você modificou:

   ```
   root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
         30
   ```

   É apresentado o valor atual da profundidade da fila.

Hosts Linux para QLogic HBA

Você pode atualizar a profundidade da fila de dispositivos de um driver QLogic em um host Linux. Para tornar as atualizações persistentes nas reinicializações, você deve criar uma nova imagem de disco RAM e reinicializar o host. Você pode usar a interface de linha de comando (CLI) do QLogic HBA para modificar a profundidade da fila do QLogic HBA.

Esta tarefa mostra como utilizar a CLI do QLogic HBA para modificar a profundidade da fila do QLogic HBA

Passos

1. Identificar o parâmetro de profundidade da fila do dispositivo a ser modificado:

   ```
   modinfo qla2xxx | grep ql2xmaxqdepth
   ```

   Você pode modificar apenas o `ql2xmaxqdepth` parâmetro de profundidade da fila, que indica a profundidade máxima da fila que pode ser definida para cada LUN. O valor padrão é 64 para RHEL 7,5 e posterior. O valor padrão é 32 para RHEL 7,4 e anterior.

   ```
   root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
   parm:       ql2xmaxqdepth:Maximum queue depth to set for each LUN.
   Default is 64. (int)
   ```

2. Atualize o valor de profundidade da fila do dispositivo:

   - Se você quiser tornar as modificações persistentes, execute as seguintes etapas:
     i. Atualize as profundidades da fila adicionando o parâmetro profundidade da fila ao `/etc/modprobe.conf` arquivo para um sistema Red Hat Enterprise Linux 5.x e ao `/etc/modprobe.d/scsi.conf` arquivo para um sistema Red Hat Enterprise Linux 6.x ou 7.x, ou para um sistema SUSE Linux Enterprise Server 11.x ou 12.x: `options qla2xxx ql2xmaxqdepth=new_queue_depth`
     ii. Crie uma nova imagem de disco RAM e reinicie o host para tornar as atualizações persistentes nas reinicializações.

     Para obter mais informações, consulte o "Administração do sistema" para sua versão do sistema operacional Linux.

   - Se você quiser modificar o parâmetro somente para a sessão atual, execute o seguinte comando:

     ```
     echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
     ```

     No exemplo a seguir, a profundidade da fila é definida como 128.

   ```
   echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
   ```

3. Verifique se os valores de profundidade da fila estão atualizados:

   ```
   cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth
   ```

   É apresentado o valor atual da profundidade da fila.

4. Modifique a profundidade da fila do QLogic HBA atualizando o parâmetro do firmware `Execution Throttle` a partir do BIOS do QLogic HBA.

   a. Inicie sessão na CLI de gestão do QLogic HBA:

      `/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli`

   b. No menu principal, selecione a `Adapter Configuration` opção.

```
[root@localhost ~]#
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
Using config file:
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli.cfg
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
Working dir: /root

QConvergeConsole

        CLI - Version 2.2.0 (Build 15)

    Main Menu

    1:  Adapter Information
    **2:  Adapter Configuration**
    3:  Adapter Updates
    4:  Adapter Diagnostics
    5:  Monitoring
    6:  FabricCache CLI
    7:  Refresh
    8:  Help
    9:  Exit


        Please Enter Selection: 2
```

   c. Na lista de parâmetros de configuração do adaptador, selecione a `HBA Parameters` opção.

```
1:  Adapter Alias
    2:  Adapter Port Alias
    **3:  HBA Parameters**
    4:  Persistent Names (udev)
    5:  Boot Devices Configuration
    6:  Virtual Ports (NPIV)
    7:  Target Link Speed (iiDMA)
    8:  Export (Save) Configuration
    9:  Generate Reports
   10:  Personality
   11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 3
```

d. Na lista de portas HBA, selecione a porta HBA necessária.

```
Fibre Channel Adapter Configuration

    HBA Model QLE2562 SN: BFD1524C78510
      1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
      2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
    HBA Model QLE2672 SN: RFE1241G81915
      3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
      4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online


        (p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 1
```

São apresentados os detalhes da porta HBA.

e. No menu HBA Parameters (parâmetros HBA), selecione a `Display HBA Parameters` opção para visualizar o valor atual `Execution Throttle` da opção.

O valor padrão da `Execution Throttle` opção é 65535.

```
HBA Parameters Menu

=======================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
```

```
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Display HBA Parameters
    2:  Configure HBA Parameters
    3:  Restore Defaults


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 1
-----------------------------------------------------------------------
--------
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
-----------------------------------------------------------------------
--------
Connection Options             : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                      : Auto
Frame Size                     : 2048
Hard Loop ID                   : 0
Loop Reset Delay (seconds)     : 5
Enable Host HBA BIOS           : Enabled
Enable Hard Loop ID            : Disabled
Enable FC Tape Support         : Enabled
Operation Mode                 : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us)  : 0
**Execution Throttle             : 65535**
Login Retry Count              : 8
Port Down Retry Count          : 30
Enable LIP Full Login          : Enabled
Link Down Timeout (seconds)    : 30
Enable Target Reset            : Enabled
LUNs Per Target                : 128
Out Of Order Frame Assembly    : Disabled
Enable LR Ext. Credits         : Disabled
Enable Fabric Assigned WWN     : N/A

Press <Enter> to continue:
```

a. Pressione **Enter** para continuar.

b. No menu HBA Parameters (parâmetros HBA), selecione a `Configure HBA Parameters` opção para modificar os parâmetros HBA.

c. No menu Configurar parâmetros, selecione a `Execute Throttle` opção e atualize o valor deste parâmetro.

```
Configure Parameters Menu

=====================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Connection Options
    2:  Data Rate
    3:  Frame Size
    4:  Enable HBA Hard Loop ID
    5:  Hard Loop ID
    6:  Loop Reset Delay (seconds)
    7:  Enable BIOS
    8:  Enable Fibre Channel Tape Support
    9:  Operation Mode
   10:  Interrupt Delay Timer (100 microseconds)
   11:  Execution Throttle
   12:  Login Retry Count
   13:  Port Down Retry Count
   14:  Enable LIP Full Login
   15:  Link Down Timeout (seconds)
   16:  Enable Target Reset
   17:  LUNs per Target
   18:  Enable Receive Out Of Order Frame
   19:  Enable LR Ext. Credits
   20:  Commit Changes
   21:  Abort Changes


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

d. Pressione **Enter** para continuar.

e. No menu Configurar parâmetros, selecione a `Commit Changes` opção para guardar as alterações.

f. Saia do menu.

Informações sobre direitos autorais

Informações sobre marcas comerciais